Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

August 6, 2014

Virginia Information Technologies Agency

ISOAG August 2014 Agenda

I.	Welcome & Opening Remarks	Mike Watson, VITA
II.	2014 Data Breach Investigative Report	Andy Bonillo, Director of Cyber Security & Public Policy, Verizon
III.	2014 Datapoint Emails	Mike Watson, VITA
IV.	2014 IS Council Committee	Mike Watson, VITA
V.	Upcoming Events	Mike Watson, VITA
VI.	Partnership Update	Bob Baskette , VITA Michael Clark, NG

Virginia Information Technologies Agency

Andy Bonillo, Director, Cyber Security & Public Policy, Verizon "2014 Data Breach Investigative Report"

August 6, 2014

Commonwealth of VA

2014 Data Breach Investigations Report Overview

Andy Bonillo

Director - Cyber Security & Public Safety

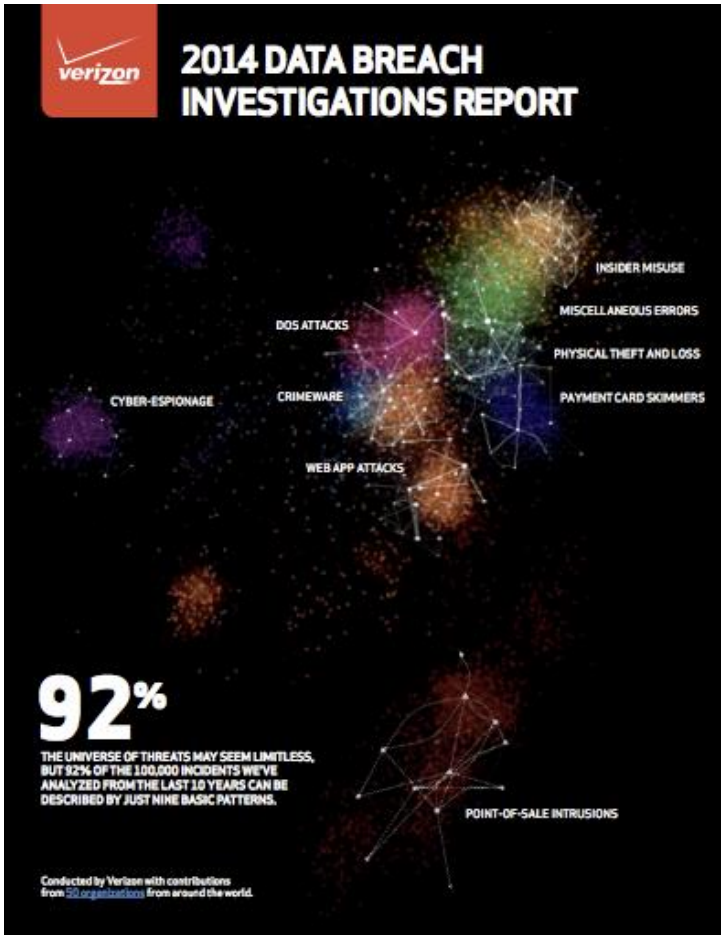
2014 DBIR by the numbers

50
CONTRIBUTING GLOBAL ORGANIZATIONS

1,367
CONFIRMED SECURITY BREACHES

63,437
SECURITY INCIDENTS

95
COUNTRIES REPRESENTED



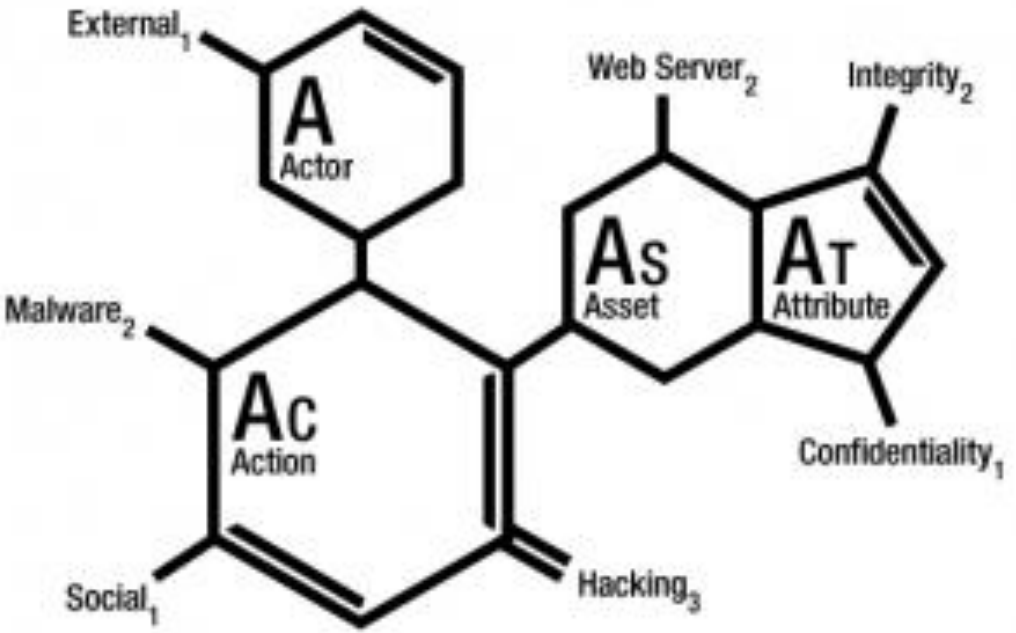
PUBLIC SECTOR

47,479
SECURITY INCIDENTS

JUST THREE INCIDENT CLASSIFICATION PATTERNS COVER 79% OF SECURITY INCIDENTS IN THE PUBLIC SECTOR.

Incidents that 50 global contributors investigated form the basis of the research

The DBIR uses the VERIS framework for data collection and analysis



Actor – Who did it?

Action – How'd they do it?

Asset – What was affected?

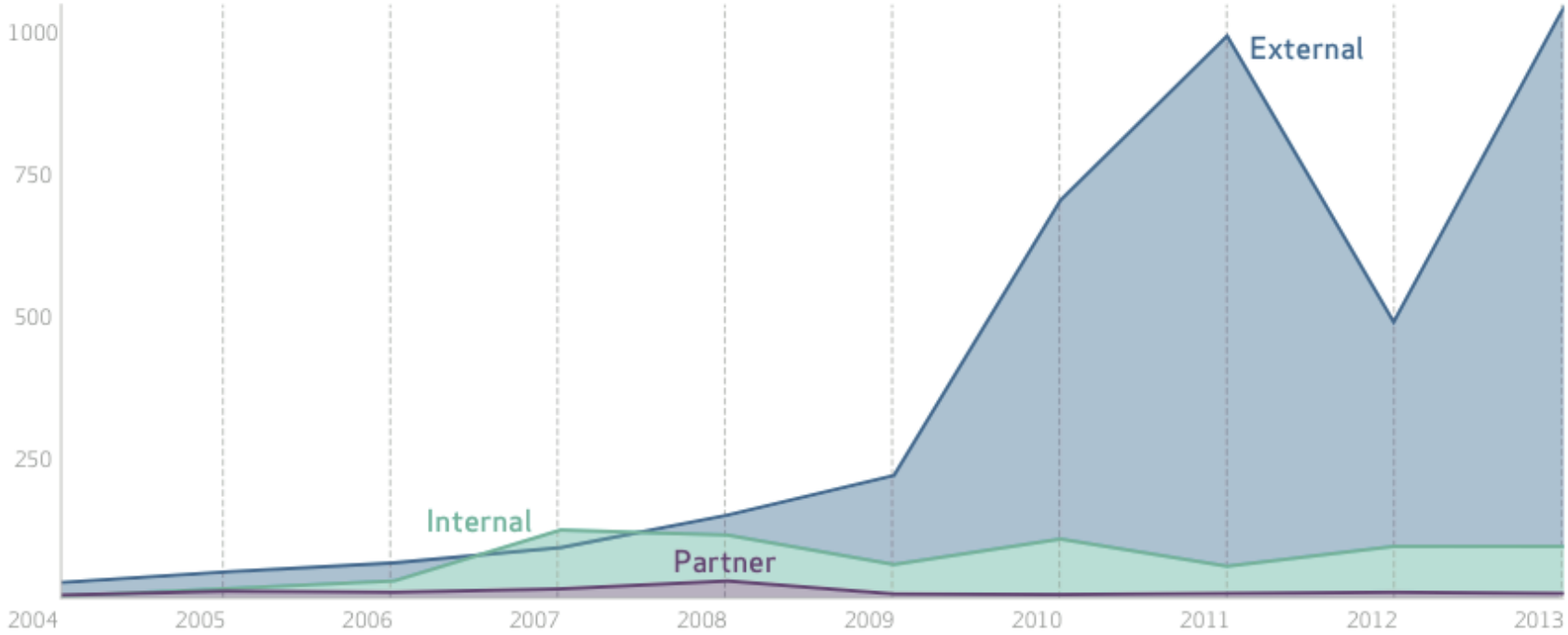
Attribute – How was it affected?

Documentation, classification examples, enumerations: http://veriscommunity.net/

A decade of data breaches

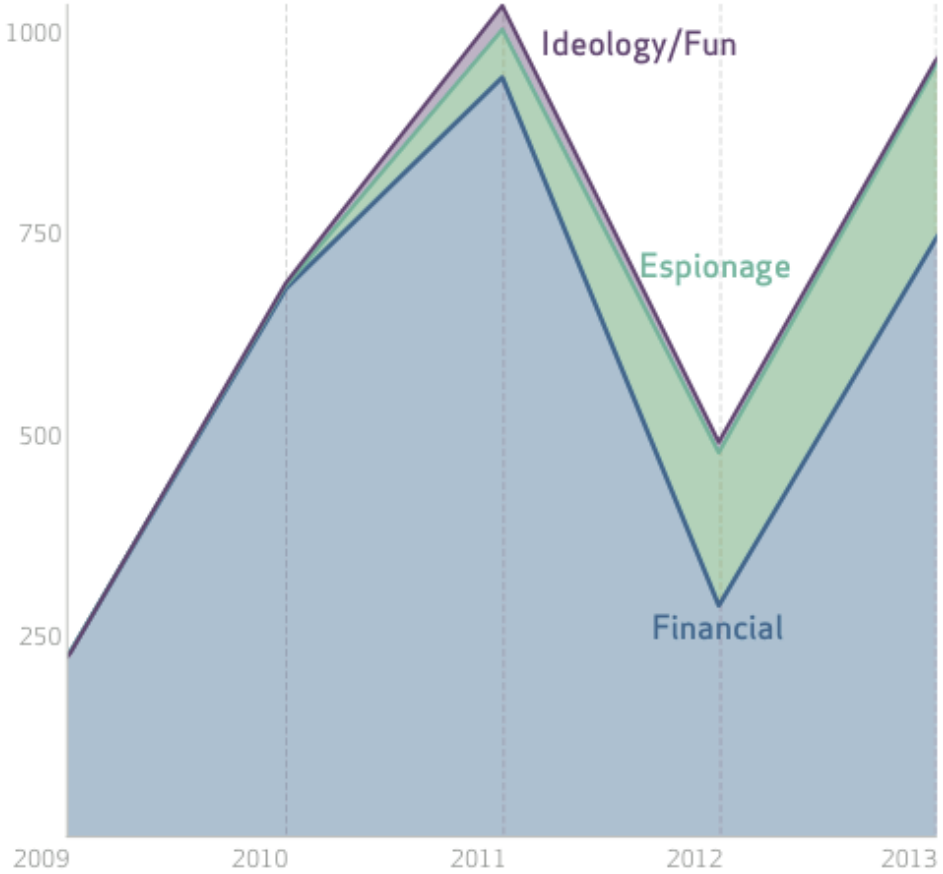
Internal and partner threat actors are fairly consistent; external ones are increasing

Figure 4.
Number of breaches per threat actor category over time



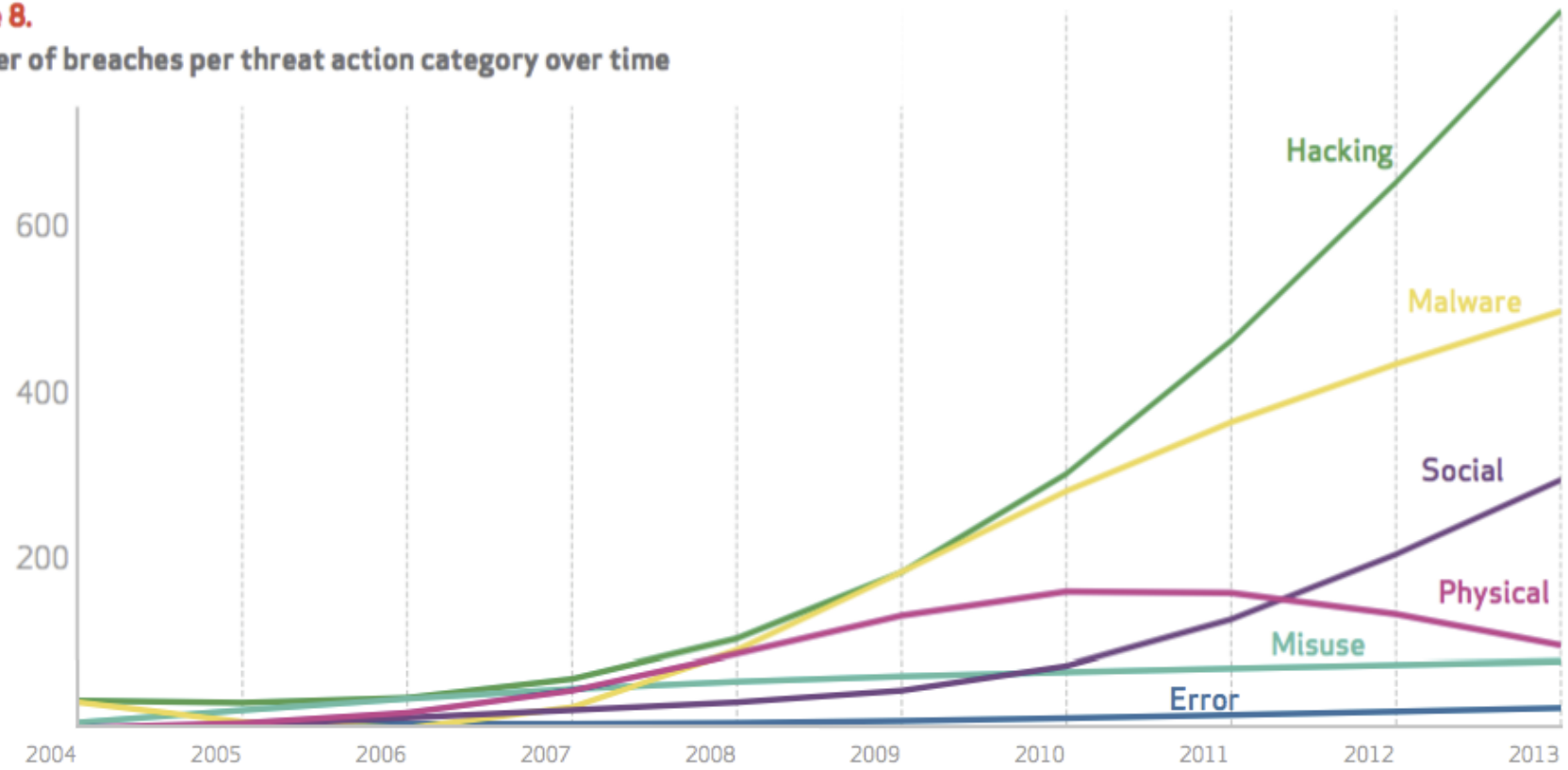
Espionage-motivated incidents increase; possibly due to increased visibility

Figure 7.
Number of breaches per threat actor motive over time



Increased threat diversity reflects both better sharing and real trends

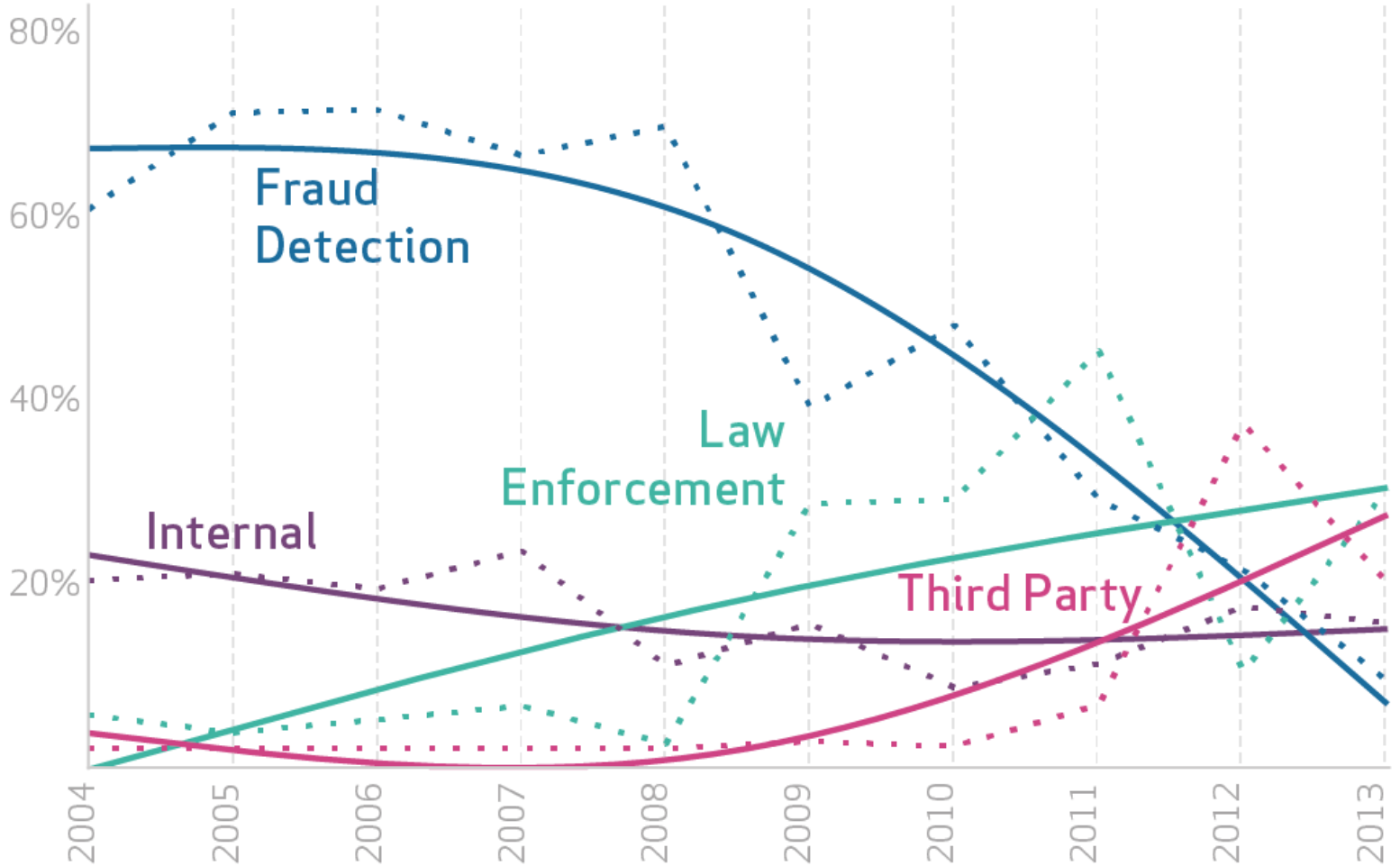
Figure 8.
Number of breaches per threat action category over time



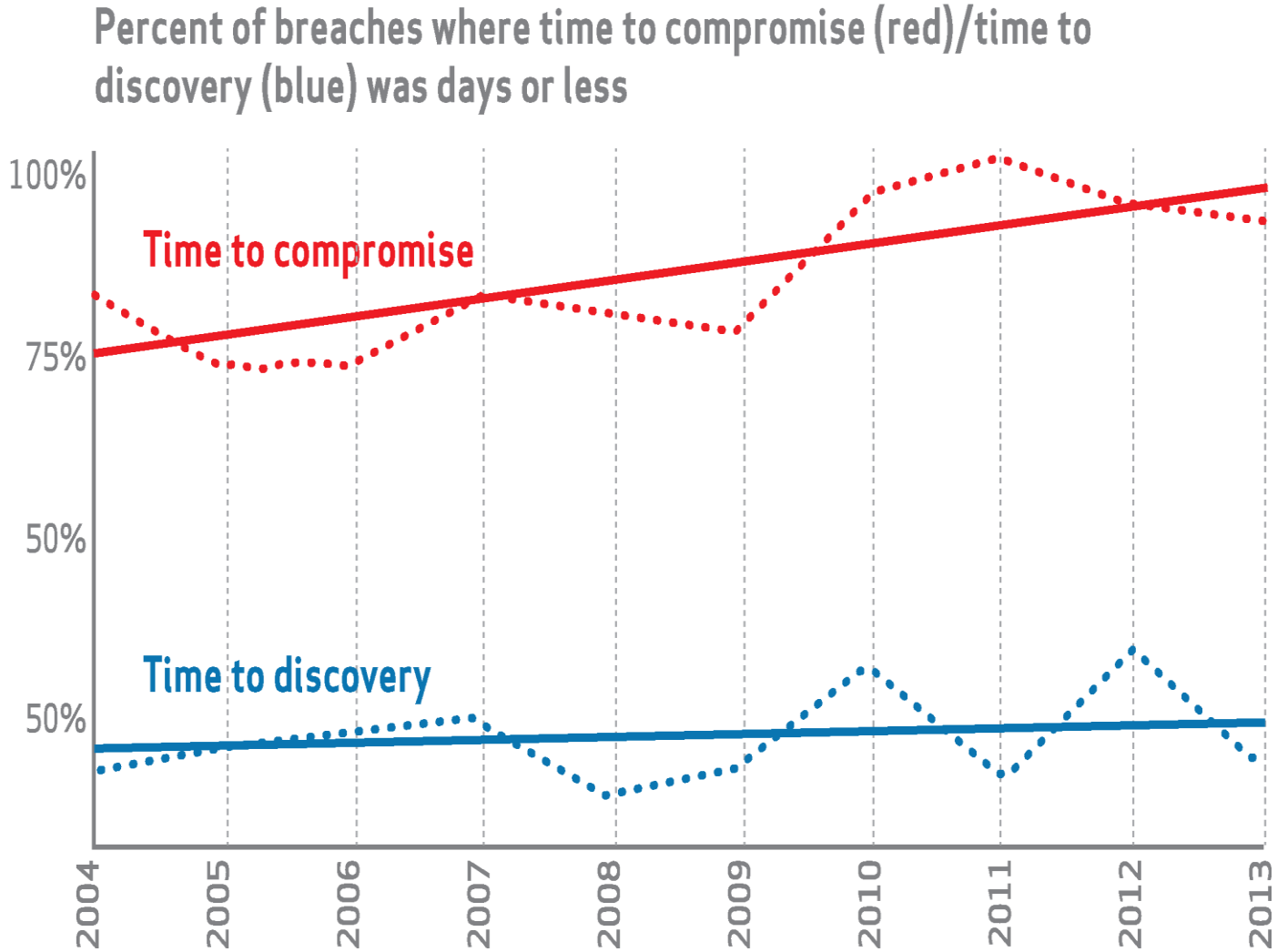
Law enforcement and third parties detect breaches more often; internal is still poor

Figure 14.

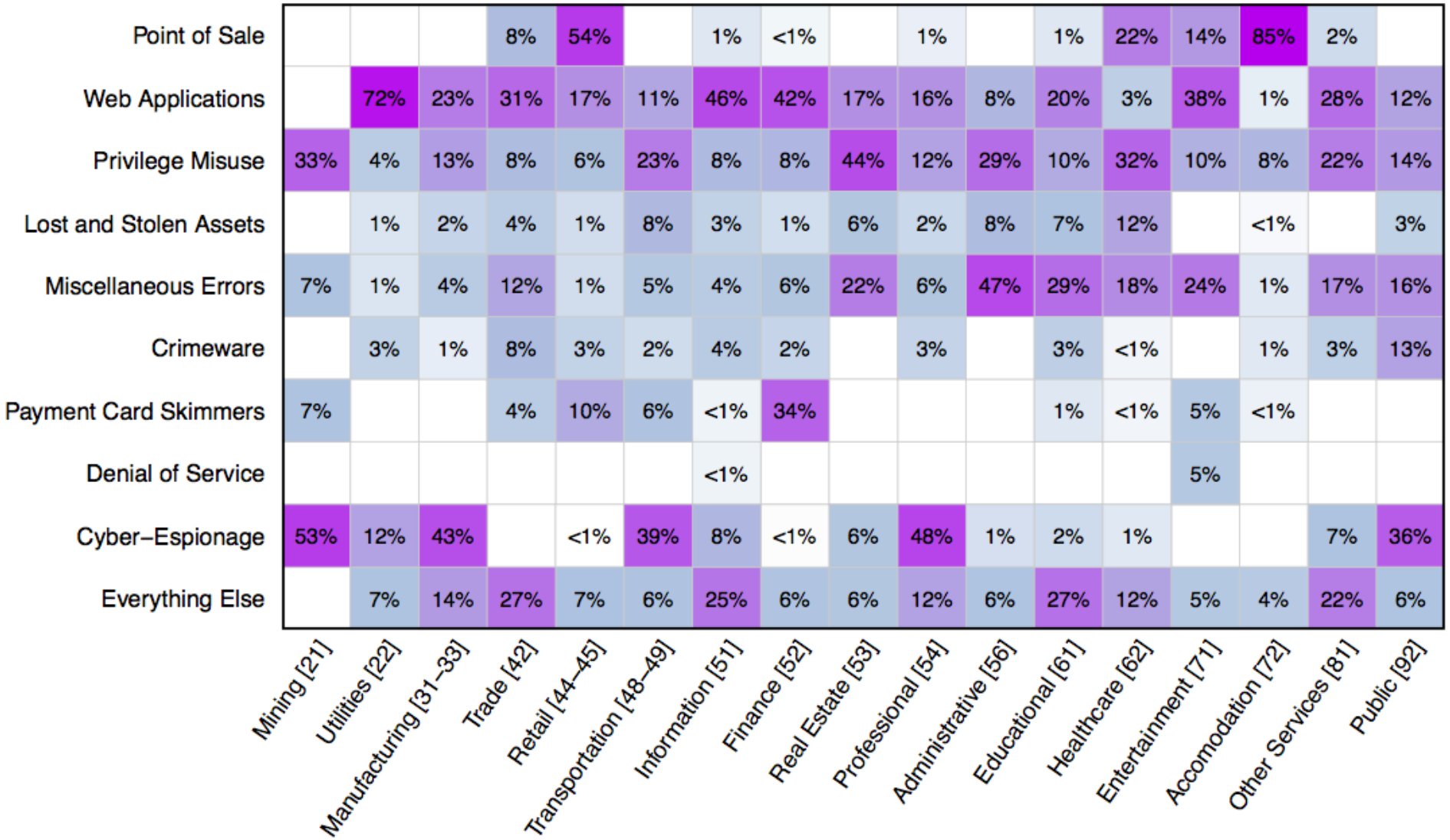
Breach discovery methods over time



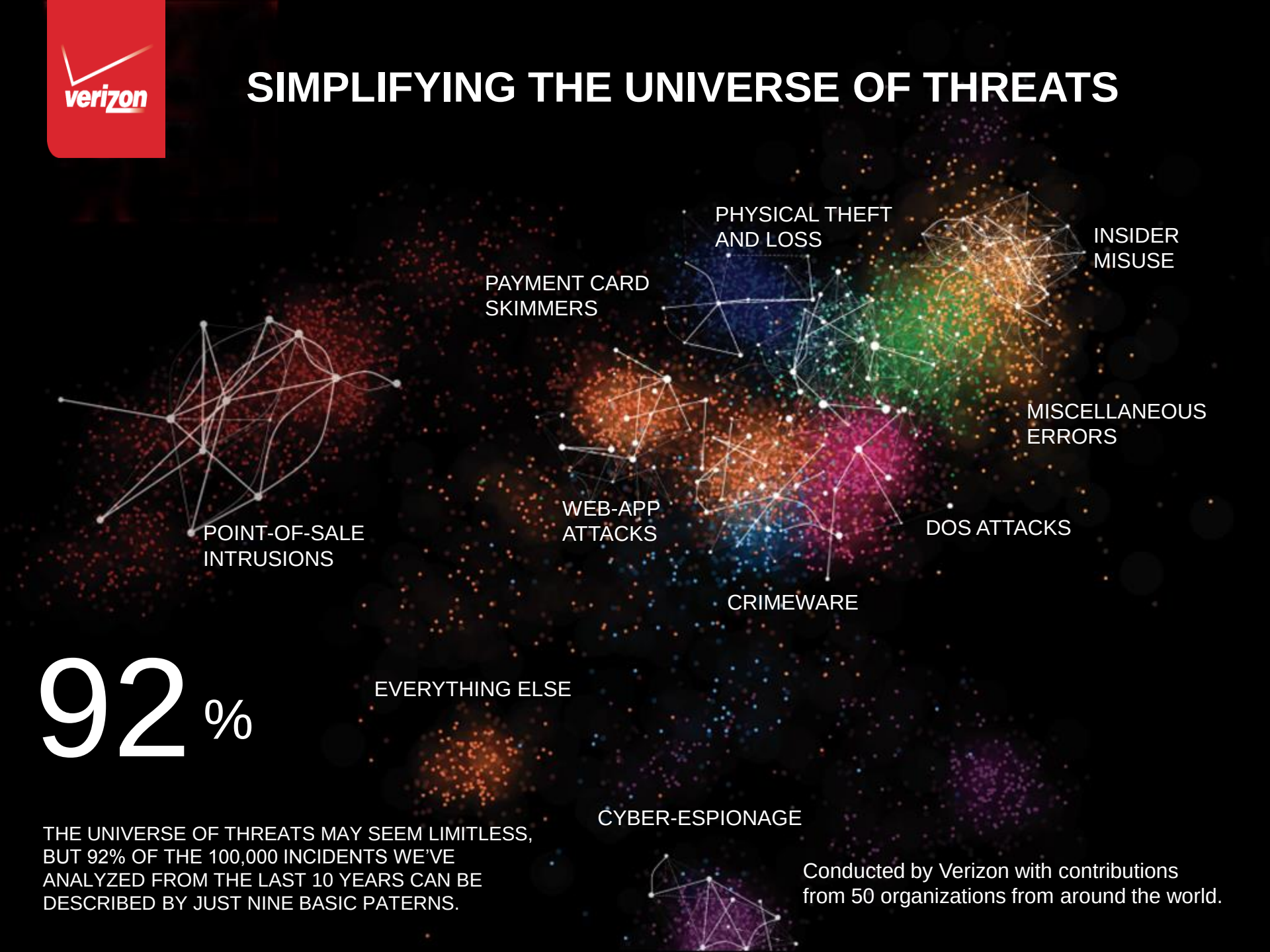
LOSING THE INNOVATION BATTLE



Same as Fig 19, but just data breaches



SIMPLIFYING THE UNIVERSE OF THREATS

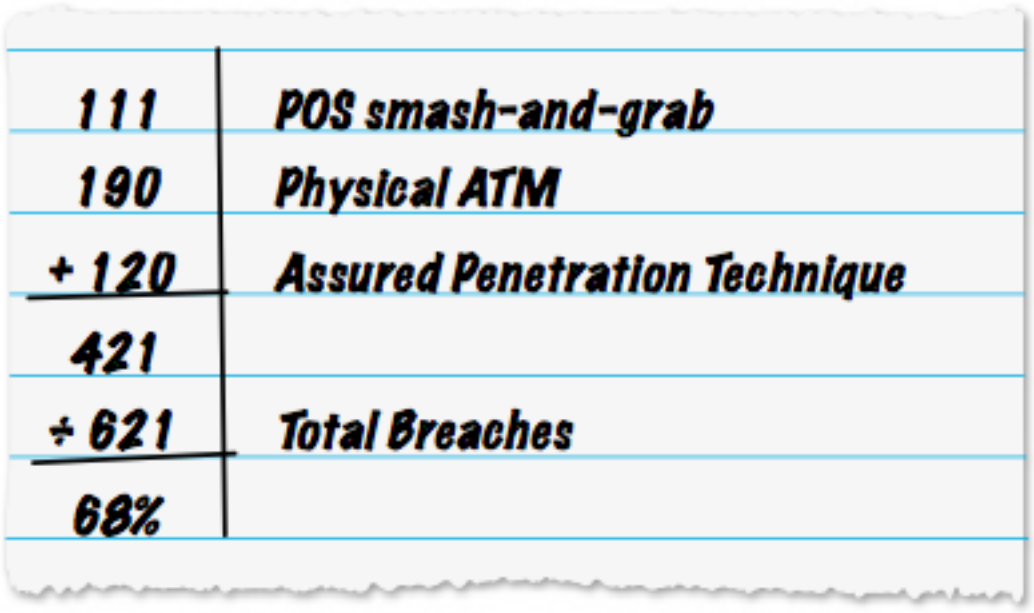


THE UNIVERSE OF THREATS MAY SEEM LIMITLESS, BUT 92% OF THE 100,000 INCIDENTS WE'VE ANALYZED FROM THE LAST 10 YEARS CAN BE DESCRIBED BY JUST NINE BASIC PATERNS.

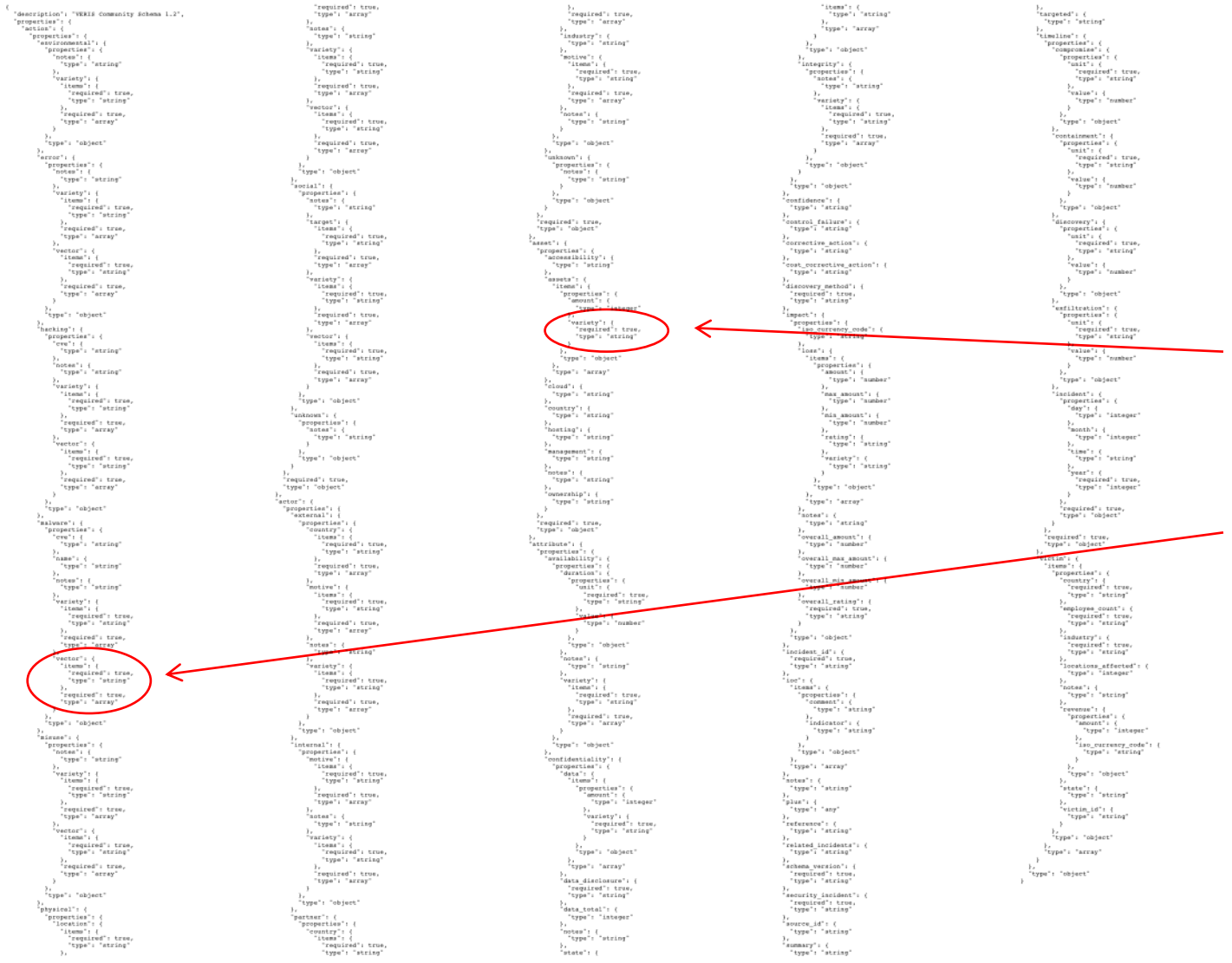
Conducted by Verizon with contributions from 50 organizations from around the world.

2014: specific patterns for specific recommendations

Last year, we noticed most breaches fit into patterns

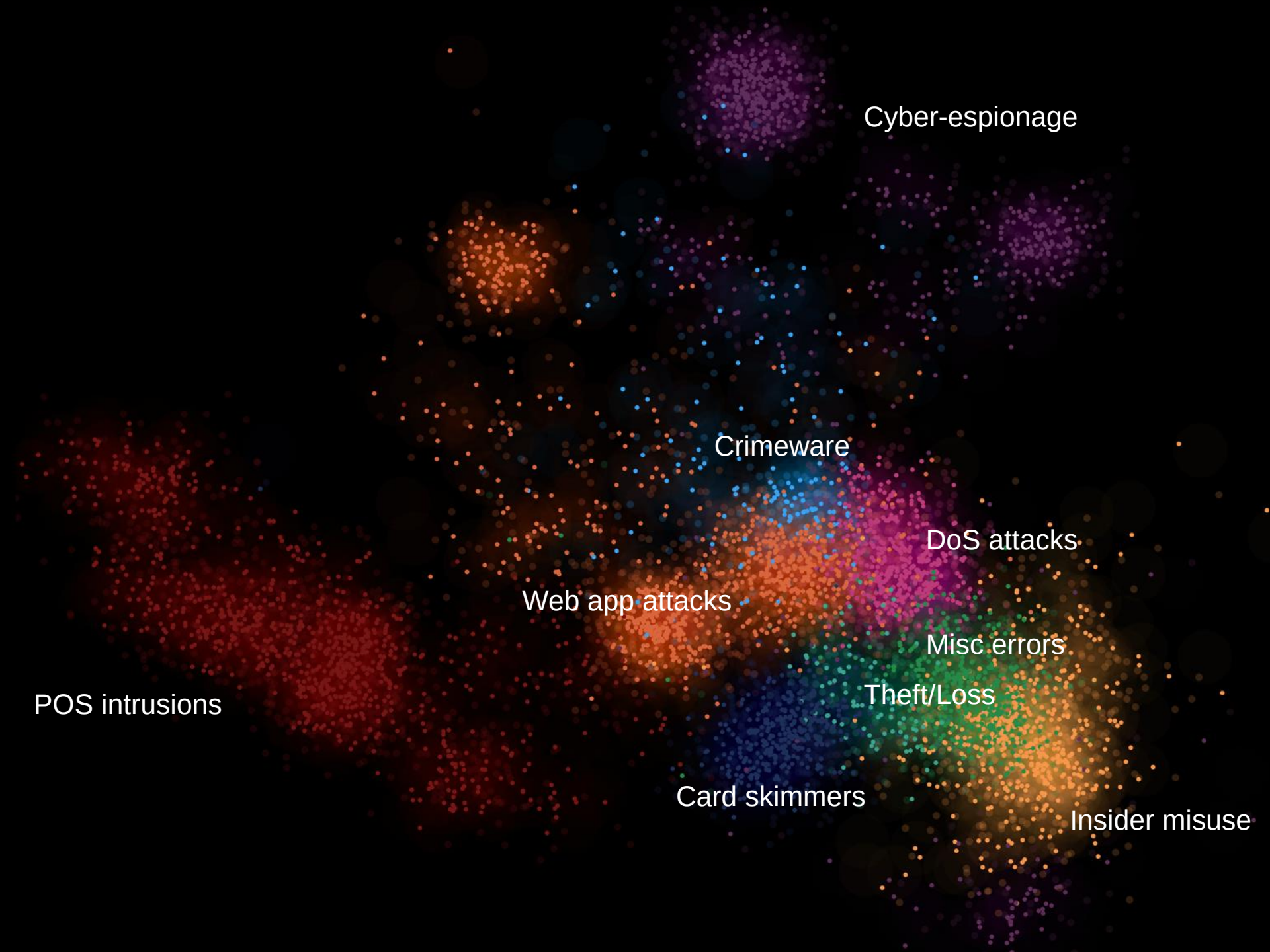


We can use the structured VERIS coding of an incident for statistical clustering



asset.variety

malware.vector


Cyber-espionage
Crimeware
DoS attacks
Web app attacks
Misc errors
Theft/Loss
POS intrusions
Card skimmers
Insider misuse

The frequency of patterns in an industry supports specific recommendations

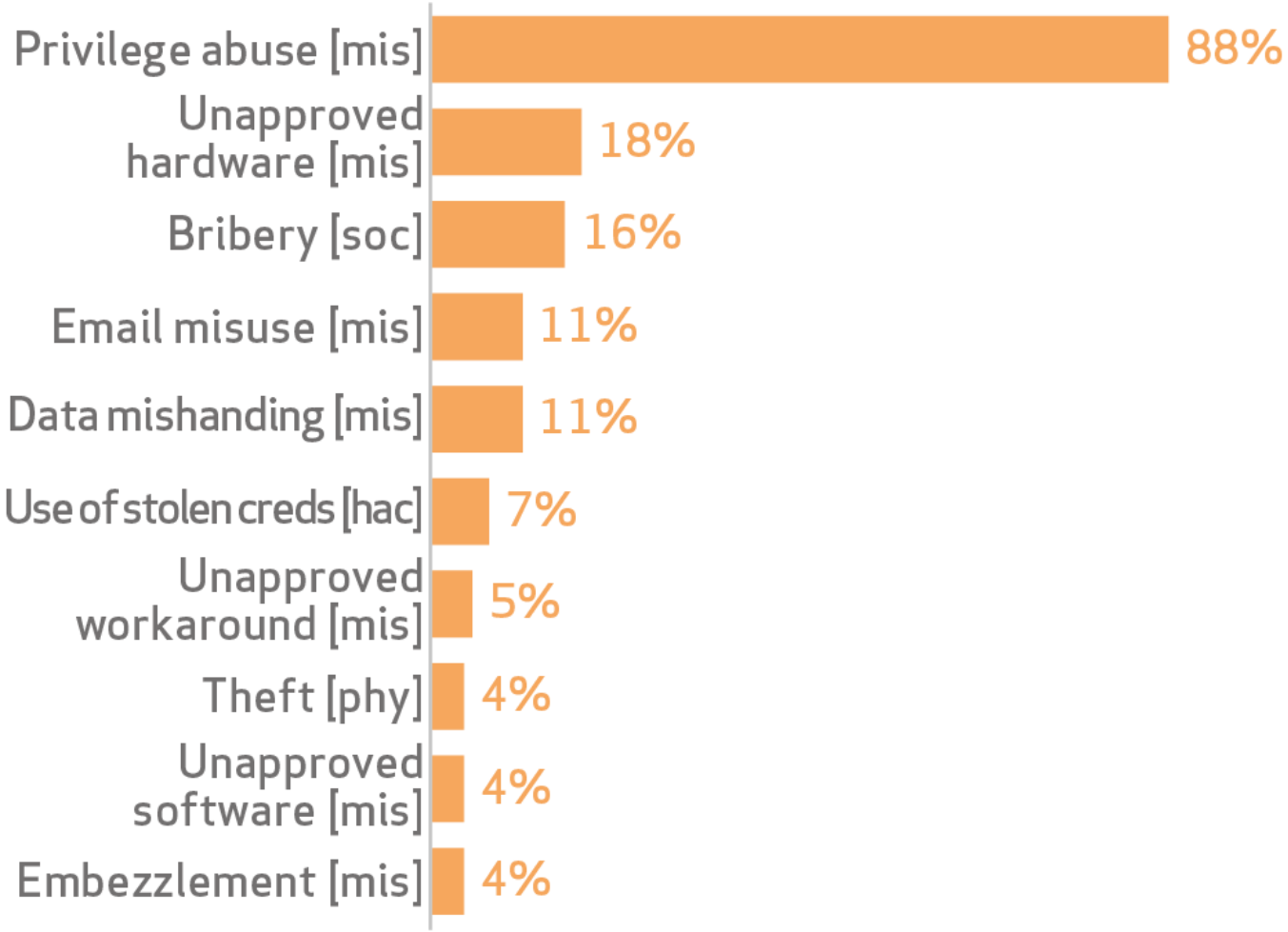
Figure 19.
Frequency of incident classification patterns per victim industry

INDUSTRY	POS INTRUS-ION	WEB APP ATTACK	INSIDER MISUSE	THEFT/ LOSS	MISC. ERROR	CRIME-WARE	PAYMENT CARD SKIMMER	DENIAL OF SERVICE	CYBER ESPION-AGE	EVERY-THING ELSE
Accommodation [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
Administrative [56]		8%	27%	12%	43%	1%		1%	1%	7%
Construction [23]	7%		13%	13%	7%	33%			13%	13%
Education [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
Entertainment [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
Finance [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
Healthcare [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
Information [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
Management [55]		11%	6%	6%	6%		11%	44%	11%	6%
Manufacturing [31,32,33]		14%	8%	4%	2%	9%		24%	30%	9%
Mining [21]			25%	10%	5%	5%	5%	5%	40%	5%
Professional [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
Public [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
Real Estate [53]		10%	37%	13%	20%	7%			3%	10%
Retail [44,45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
Trade [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
Transportation [48,49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
Utilities [22]		38%	3%	1%	2%	31%		14%	7%	3%
Other [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

Insider and privilege misuse

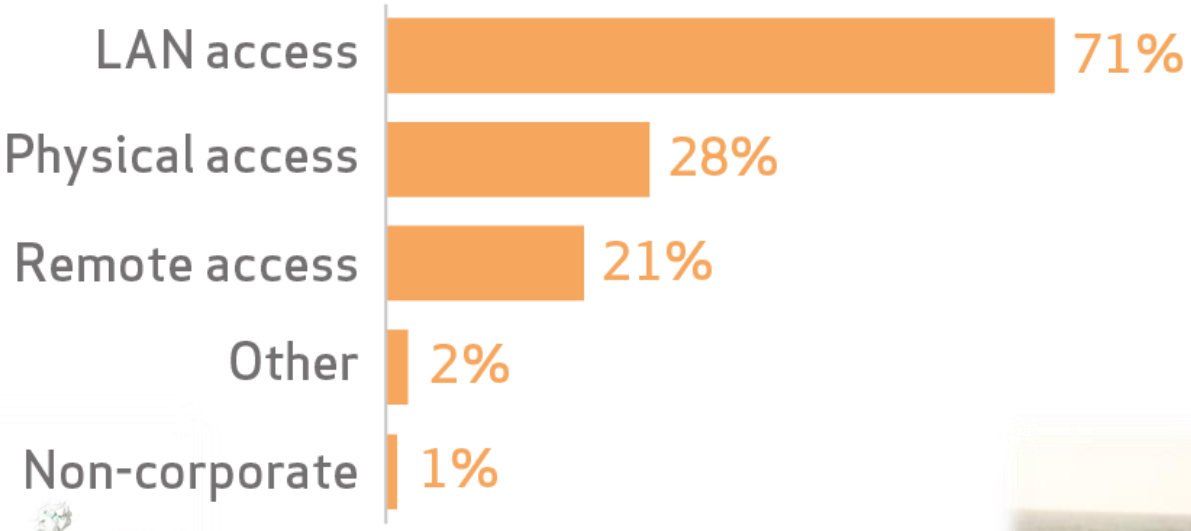
Most insider misuse activity abuses trust necessary to perform normal duties

Figure 30.
Top 10 threat action varieties within Insider Misuse (n=153)



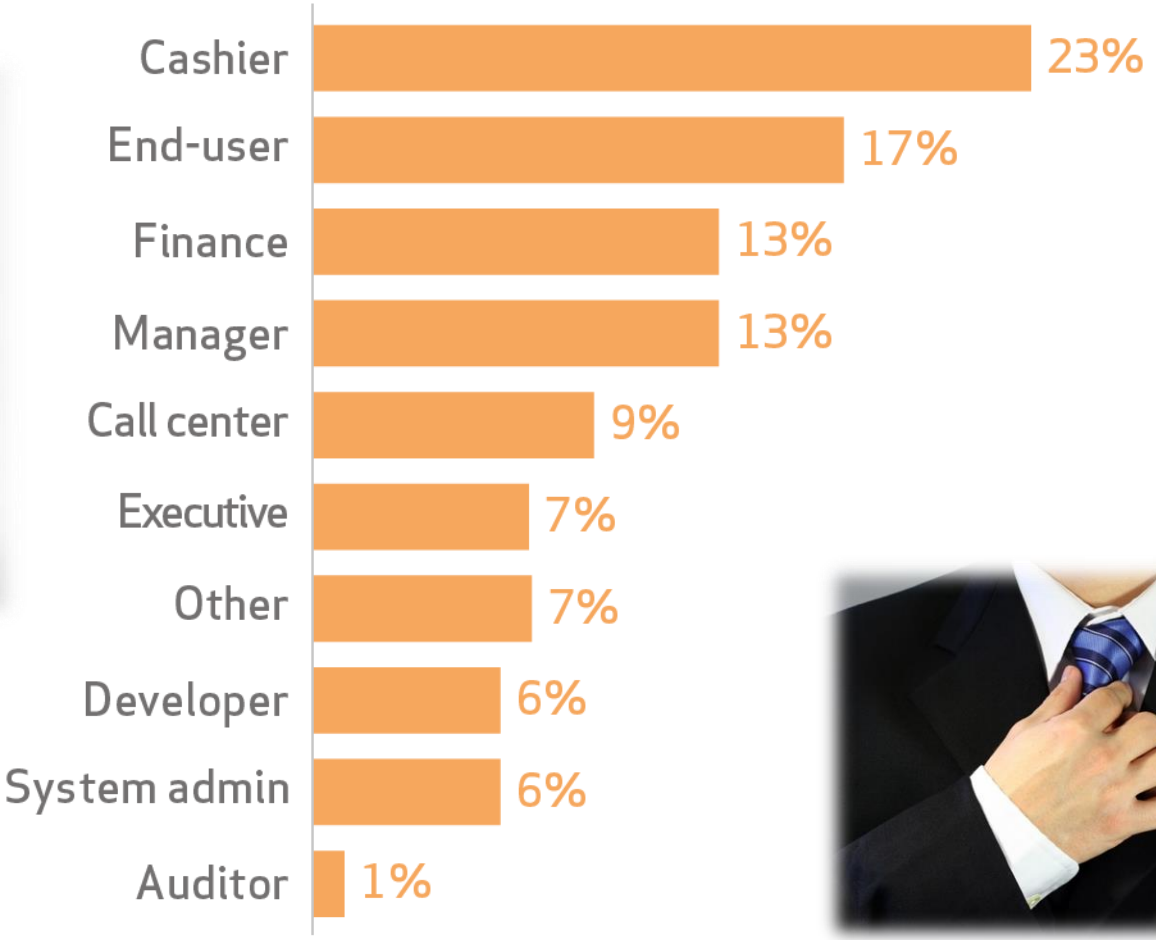
Most incidents happen at the victim organization

Figure 31.
Vector for threat actions within Insider Misuse (n=123)



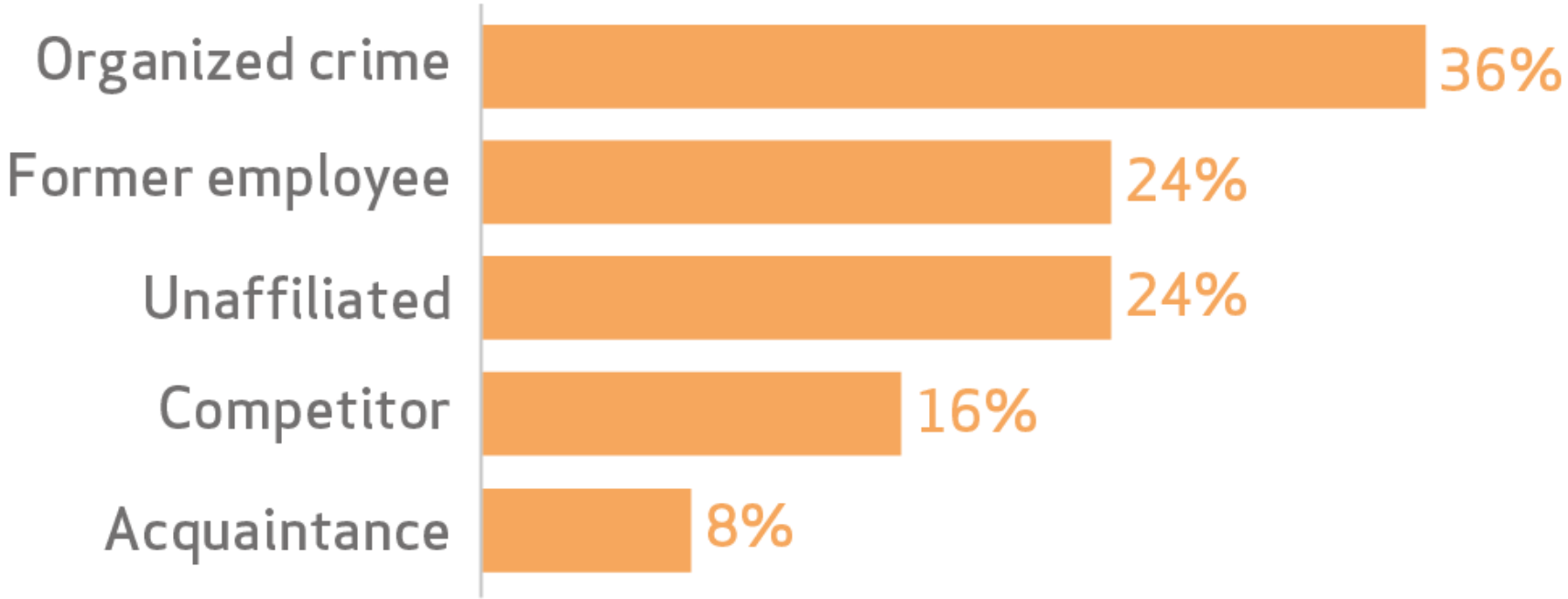
Internal actors include more managers and executives than in prior years

Figure 32.
Top 10 varieties of internal actors within Insider Misuse (n=99)



External actors bribe, exploit known access, and solicit information

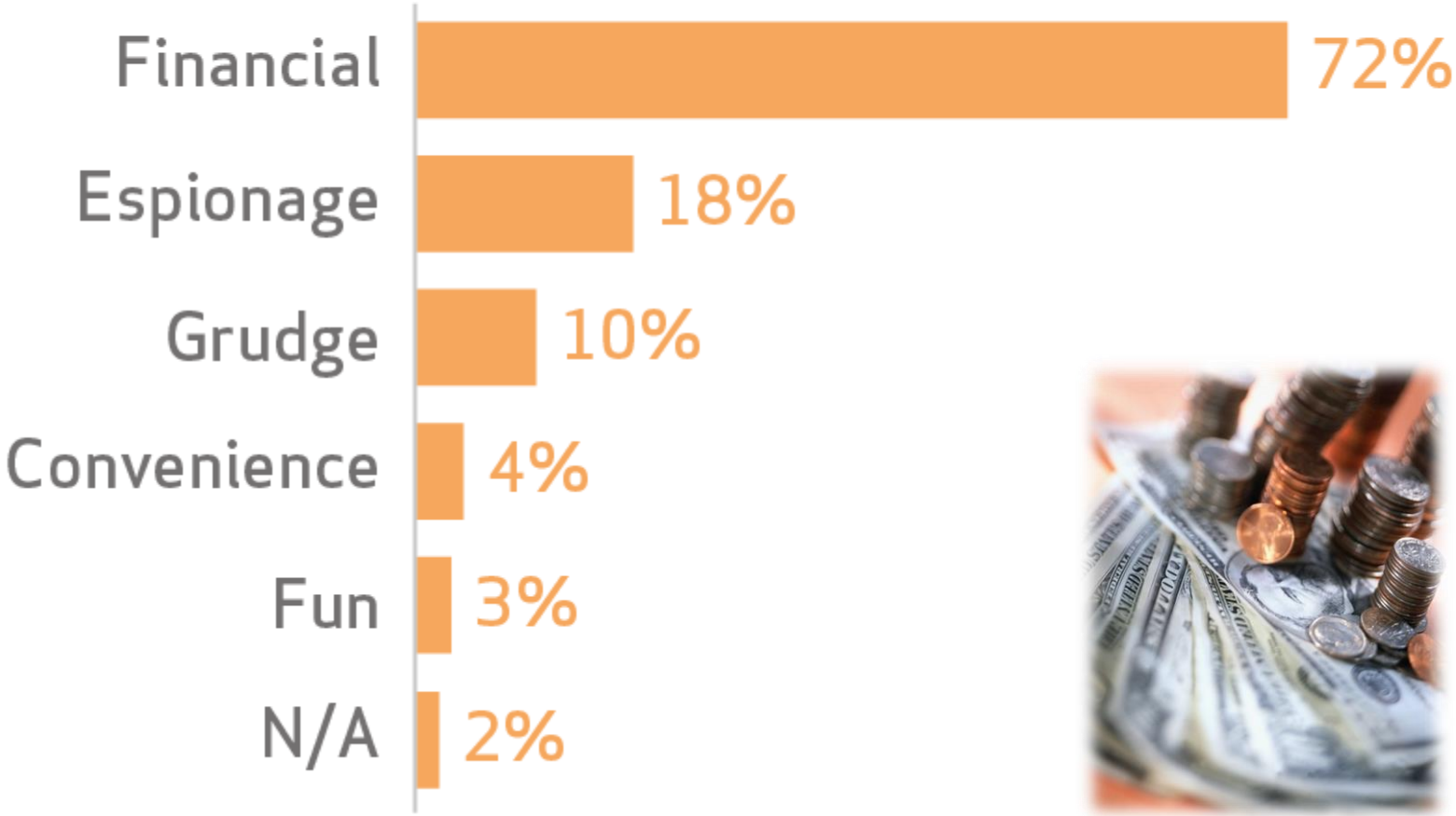
Figure 33.
Variety of external actors within Insider Misuse (n=25)



Motivation is primarily financial, with some espionage (to benefit a competitor)

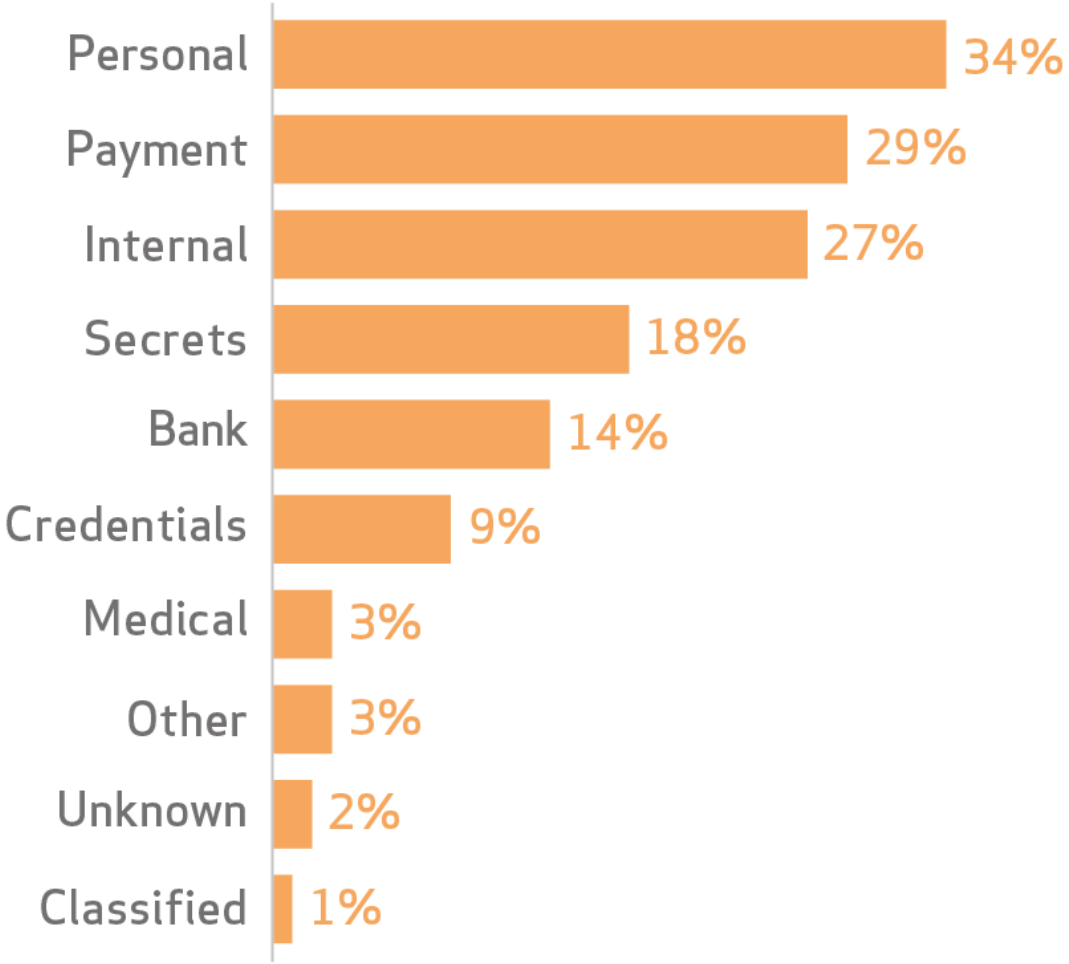
Figure 34.

Actor motives within Insider Misuse (n=125)



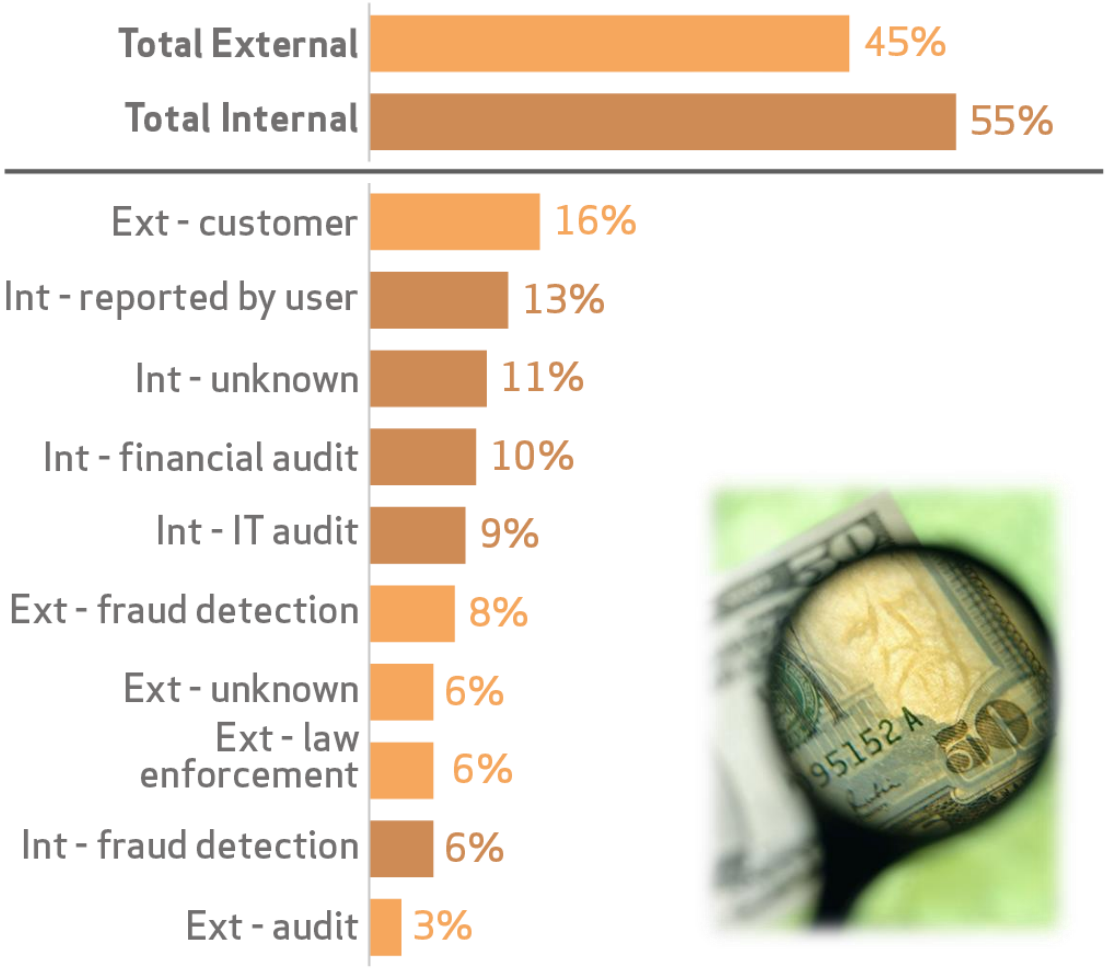
The varieties of data at risk are diverse

Figure 35.
Variety of at-risk data within Insider Misuse (n=108)



Internal detection is unusually common for insider and privilege misuse

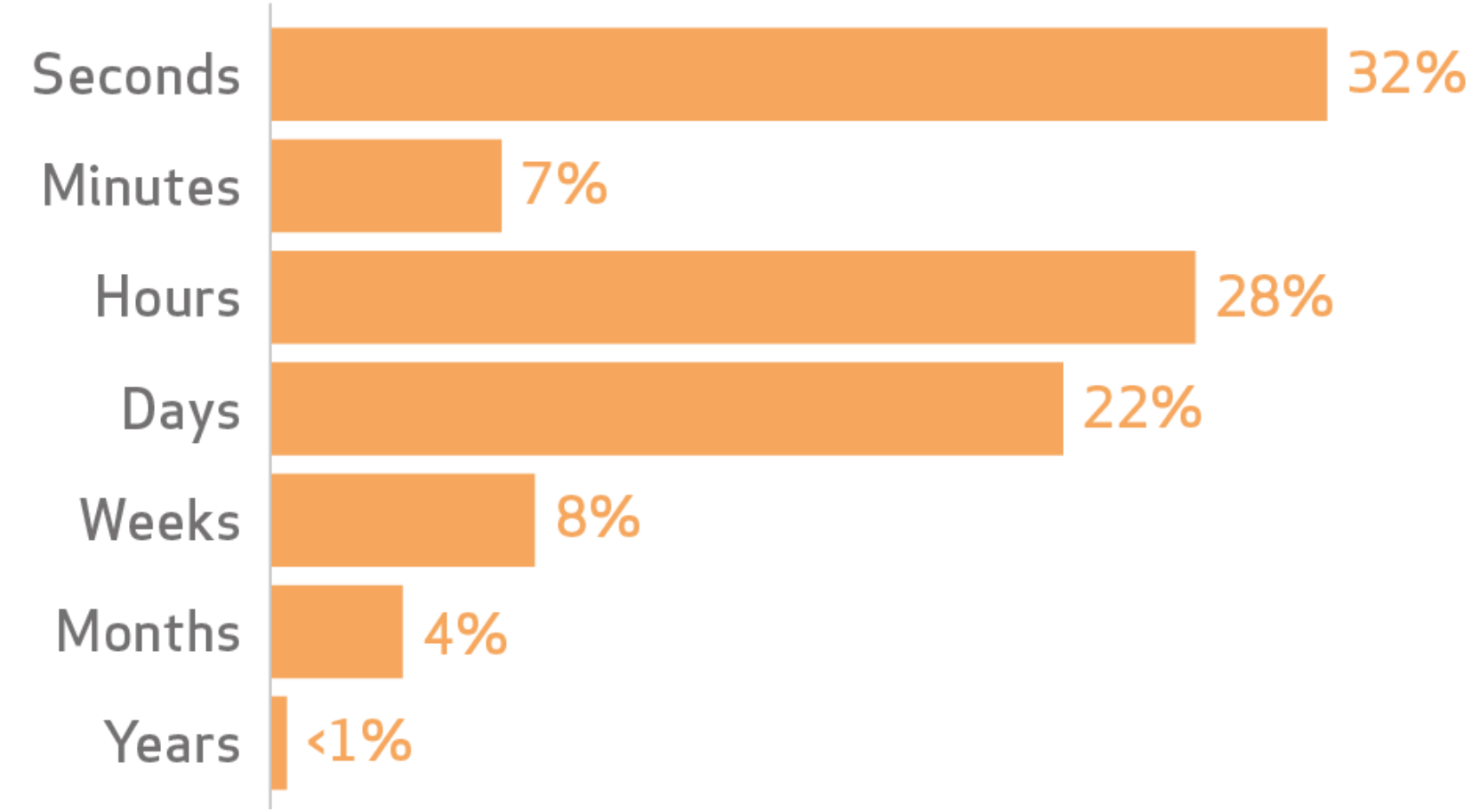
Figure 37.
Top 10 discovery methods within Insider Misuse (n=122)



Discovery time is also unusual: many were discovered within days

Figure 38.

Discovery timeline within Insider Misuse (n=1,017)



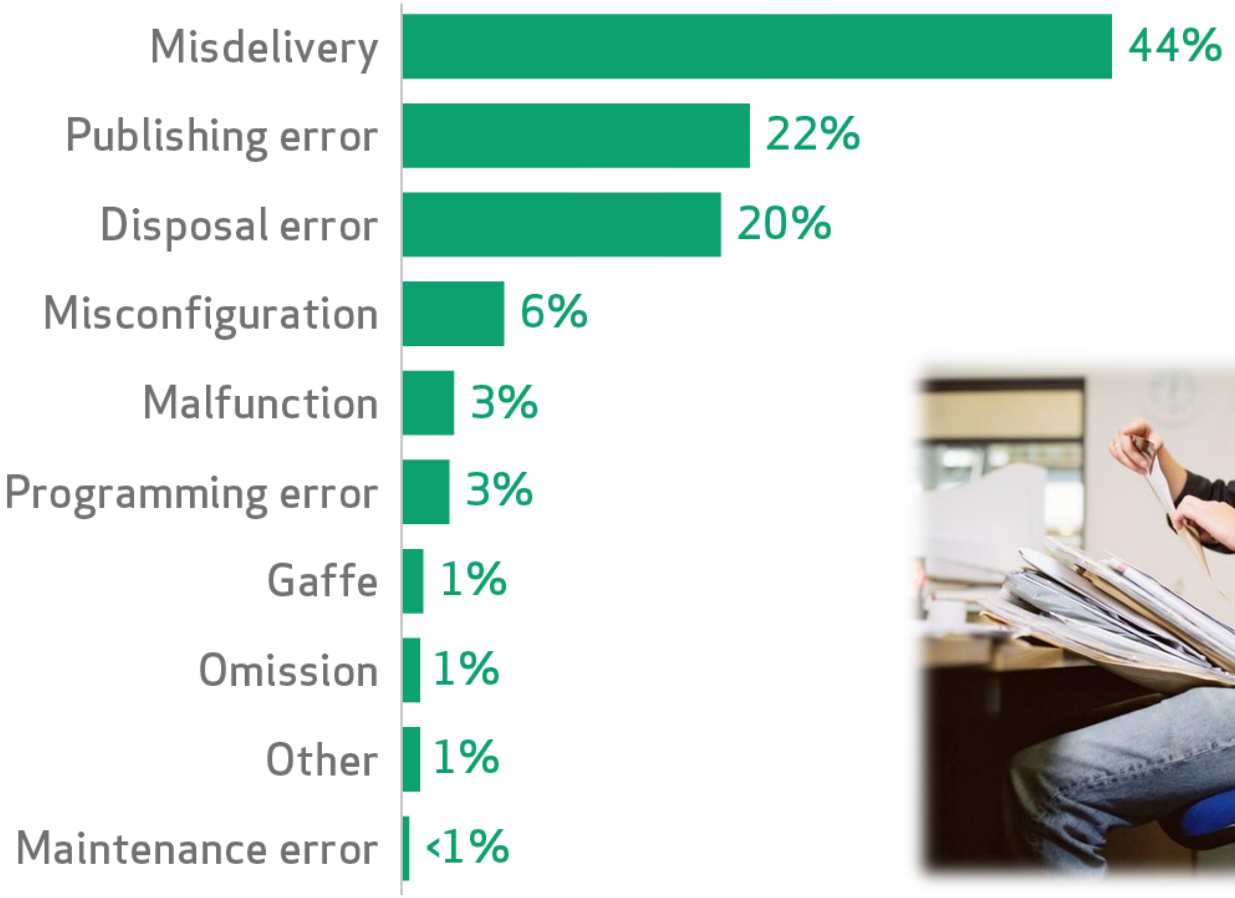
Recommended controls for insider and privilege misuse

- Know your data and who has access to it
- Review user accounts
- Watch for data exfiltration
- Publish audit results

Miscellaneous errors

Highly repetitive processes involving sensitive data are particularly error prone

Figure 43.
Top 10 threat action varieties within Miscellaneous Errors (n=558)



Discovery typically takes a long time, and it's external about two-thirds of the time

Figure 45.
Discovery and containment timeline within Miscellaneous Errors

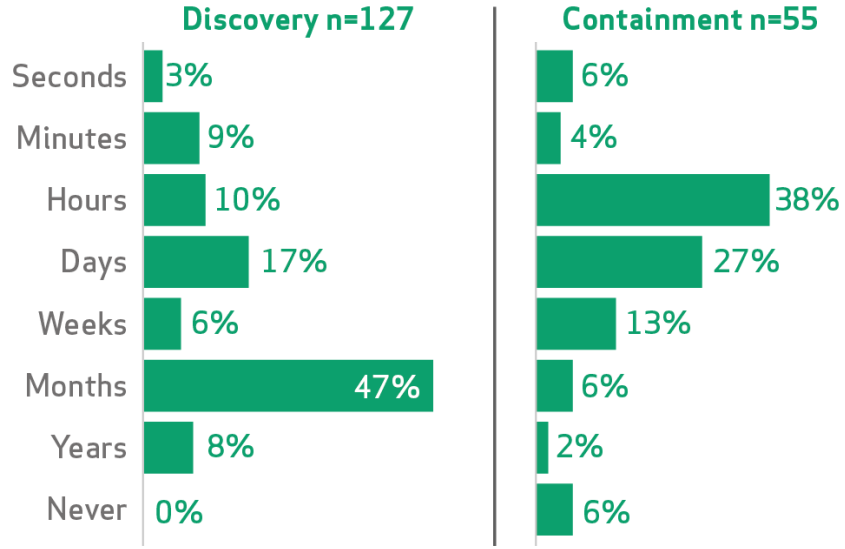
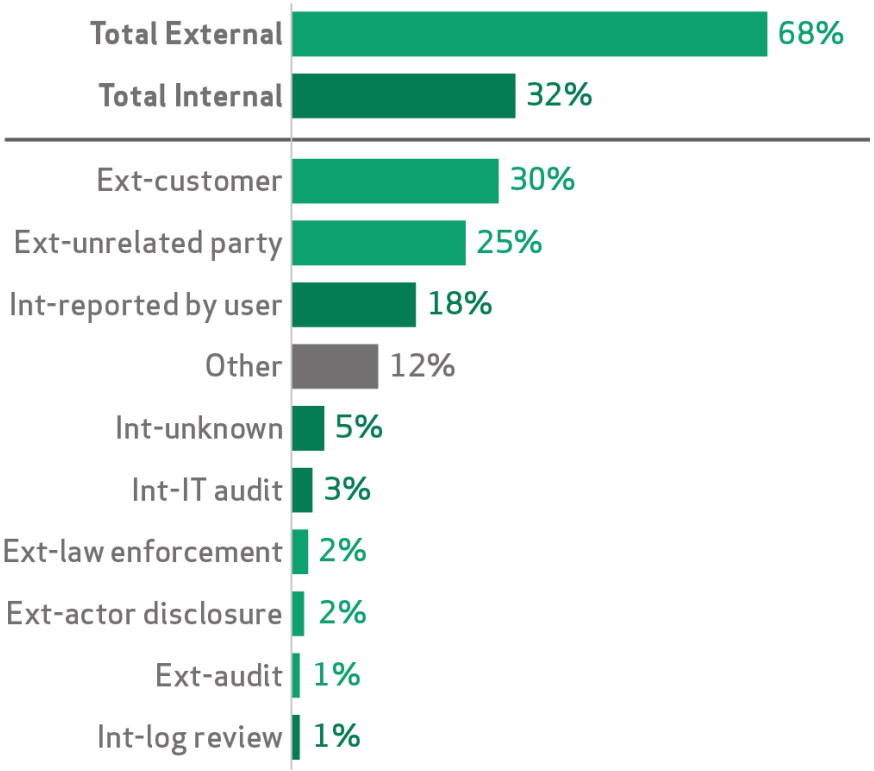


Figure 46.
Top 10 discovery methods for Miscellaneous Error incidents (n=148)



Recommended controls for miscellaneous errors

- Consider Data Loss Prevention (DLP) software
- Tighten processes around posting documents
- Spot-check large mailings
- IT disposes of all information assets (and test them)

Cyber espionage

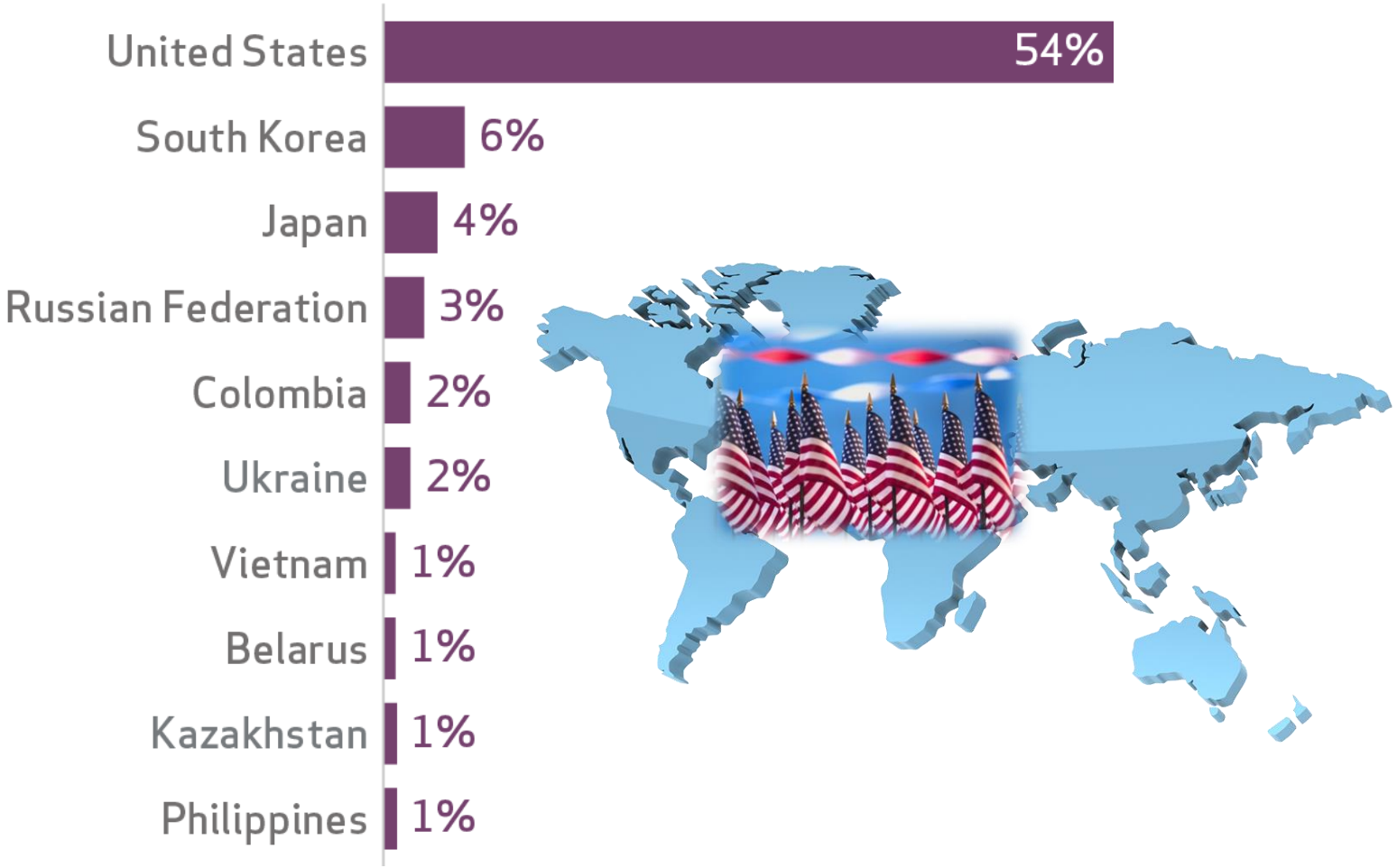
Certain industries saw far more cyber espionage than others

Figure 56.
Number of incidents by victim industry and size within Cyber-espionage

Industry	Total	Small	Large	Unknown
Administrative [56]	2	1	1	0
Construction [23]	1	0	0	1
Education [61]	2	1	1	0
Finance [52]	3	0	2	1
Healthcare [62]	2	1	0	1
Information [51]	11	2	2	7
Management [55]	2	1	1	0
Manufacturing [31,32,33]	81	5	17	59
Mining [21]	5	0	2	3
Professional [54]	114	11	5	98
Public [92]	133	20	19	94
Real Estate [53]	1	1	0	0
Retail [44,45]	1	0	1	0
Transportation [48,49]	5	1	3	1
Utilities [22]	8	0	1	7
Other [81]	5	5	0	0
Unknown	135	0	3	132
Total	**511**	**49**	**58**	**404**

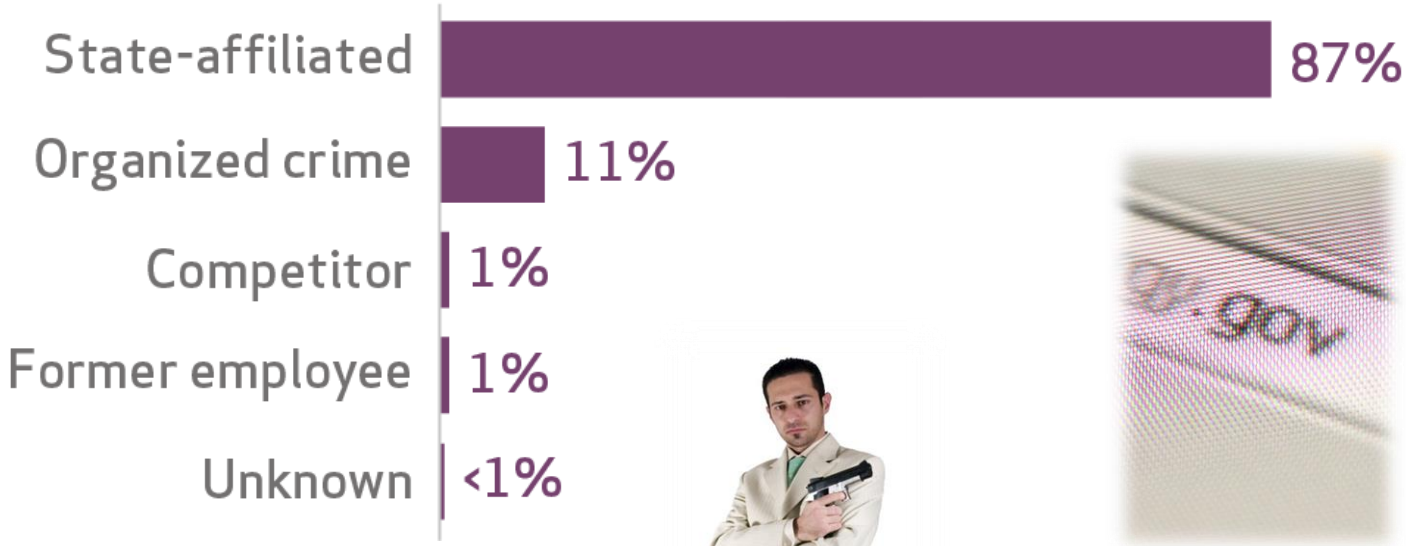
About half of our sample is U.S. victims, but visibility on others is increasing

Figure 57.
Victim country within Cyber-espionage (n=470)



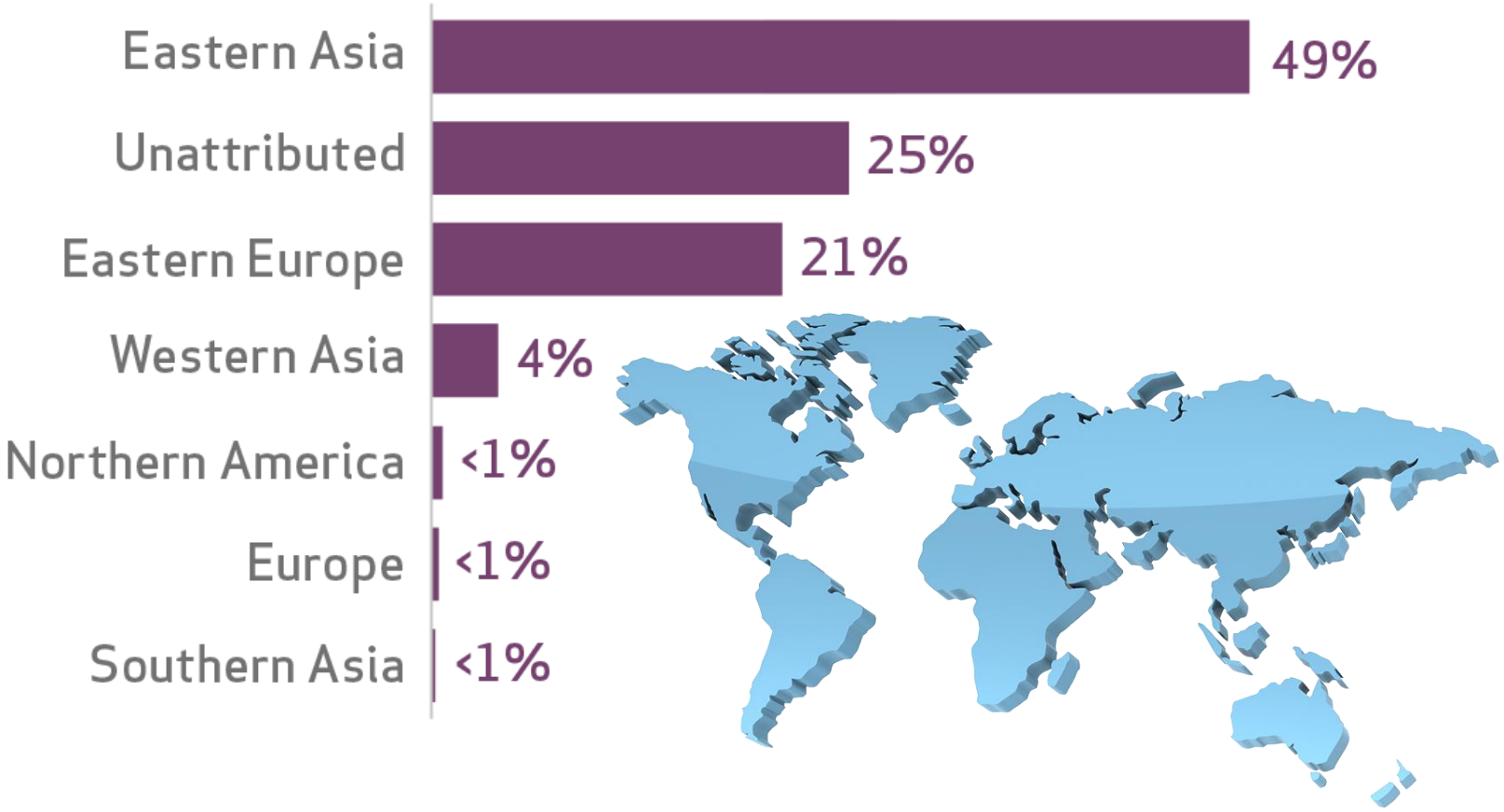
Most actors are state affiliated, but a significant minority are not

Figure 58.
Variety of external actors within Cyber-espionage (n=437)



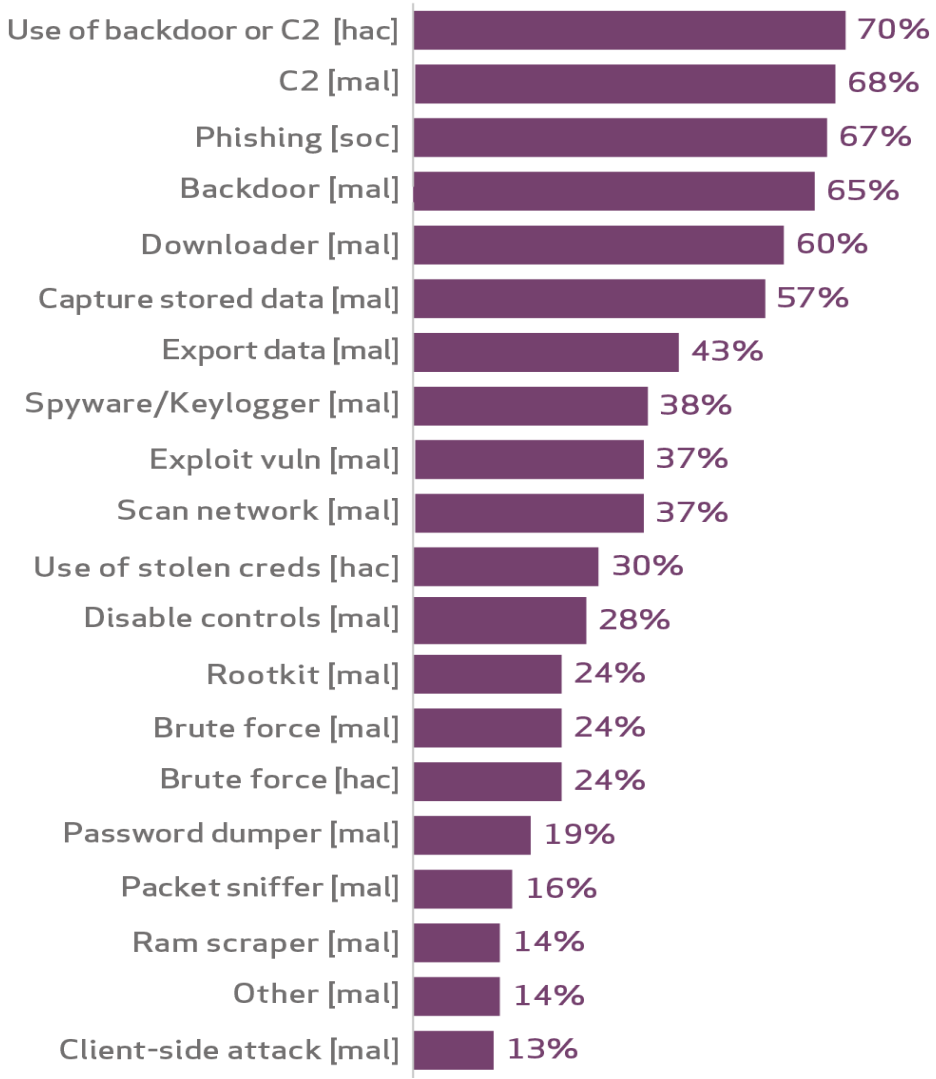
More data about non-eastern-Asia actors reflects more, better research

Figure 59.
Region of external actors within Cyber-espionage (n=230)



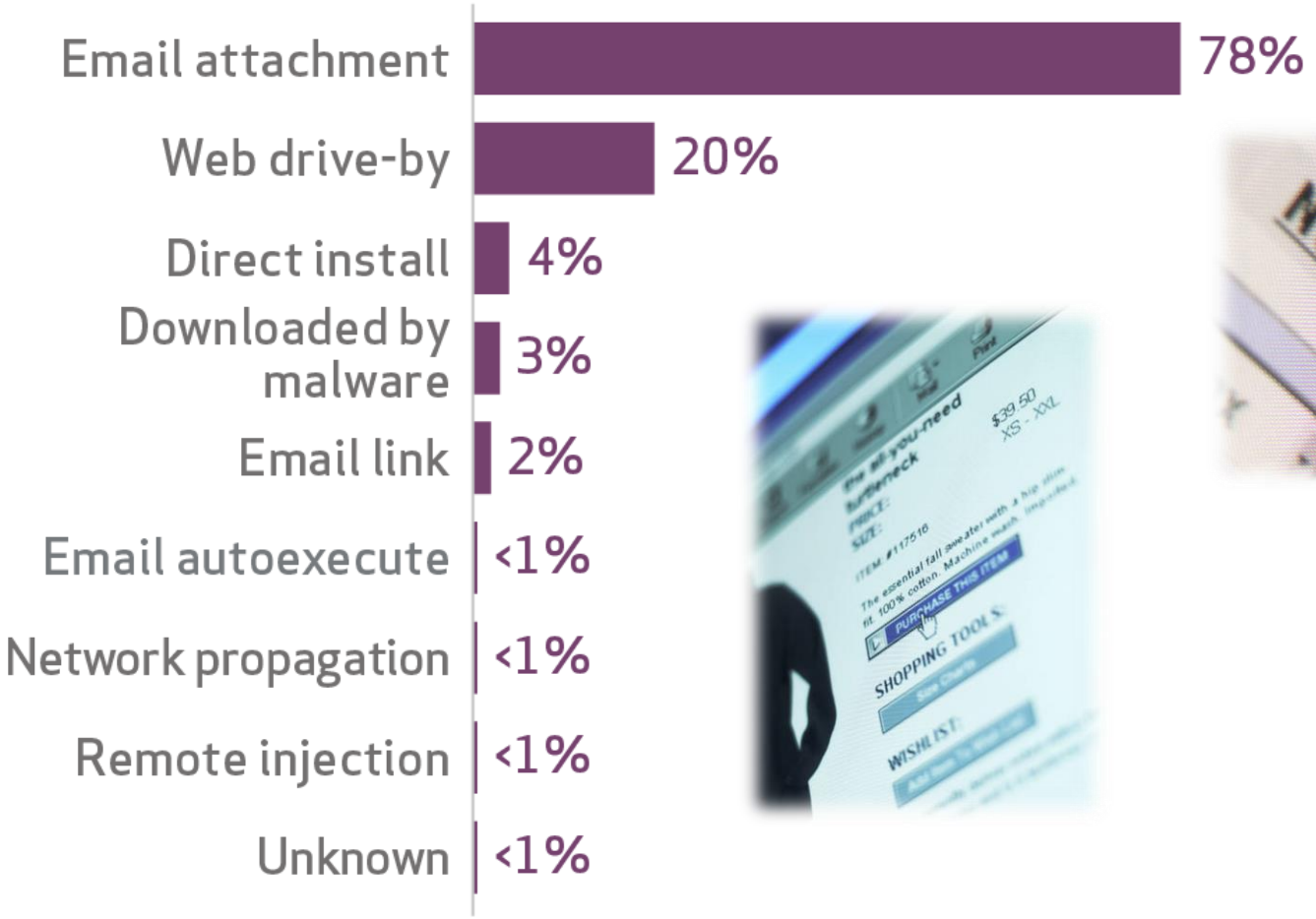
Cyber espionage involves a much wider range of tools than other patterns

Figure 60.
Top threat action varieties within Cyber-espionage (n=426)

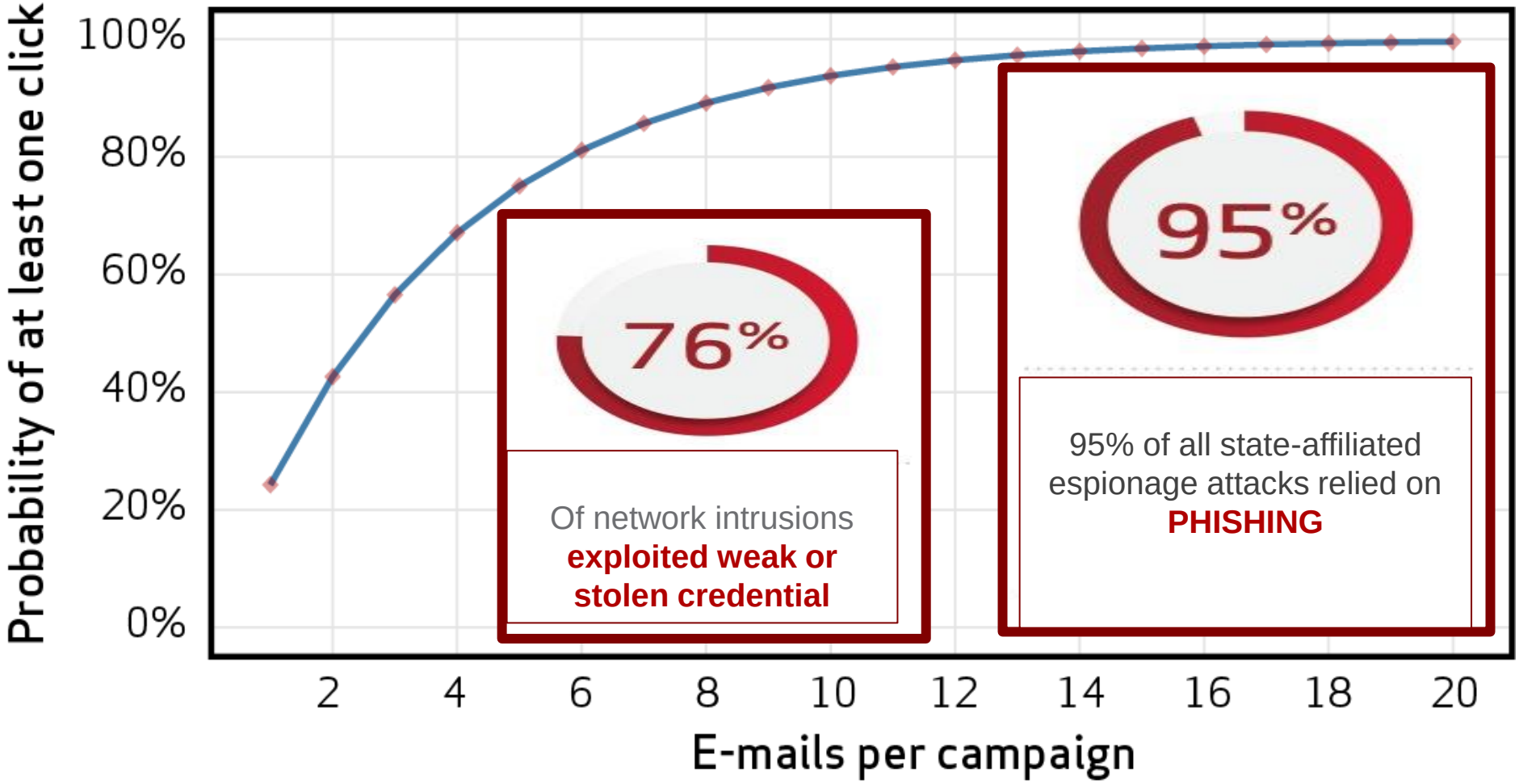


But there are relatively few ways attackers gain access to victims

Figure 61.
Vector for malware actions within Cyber-espionage (n=329)



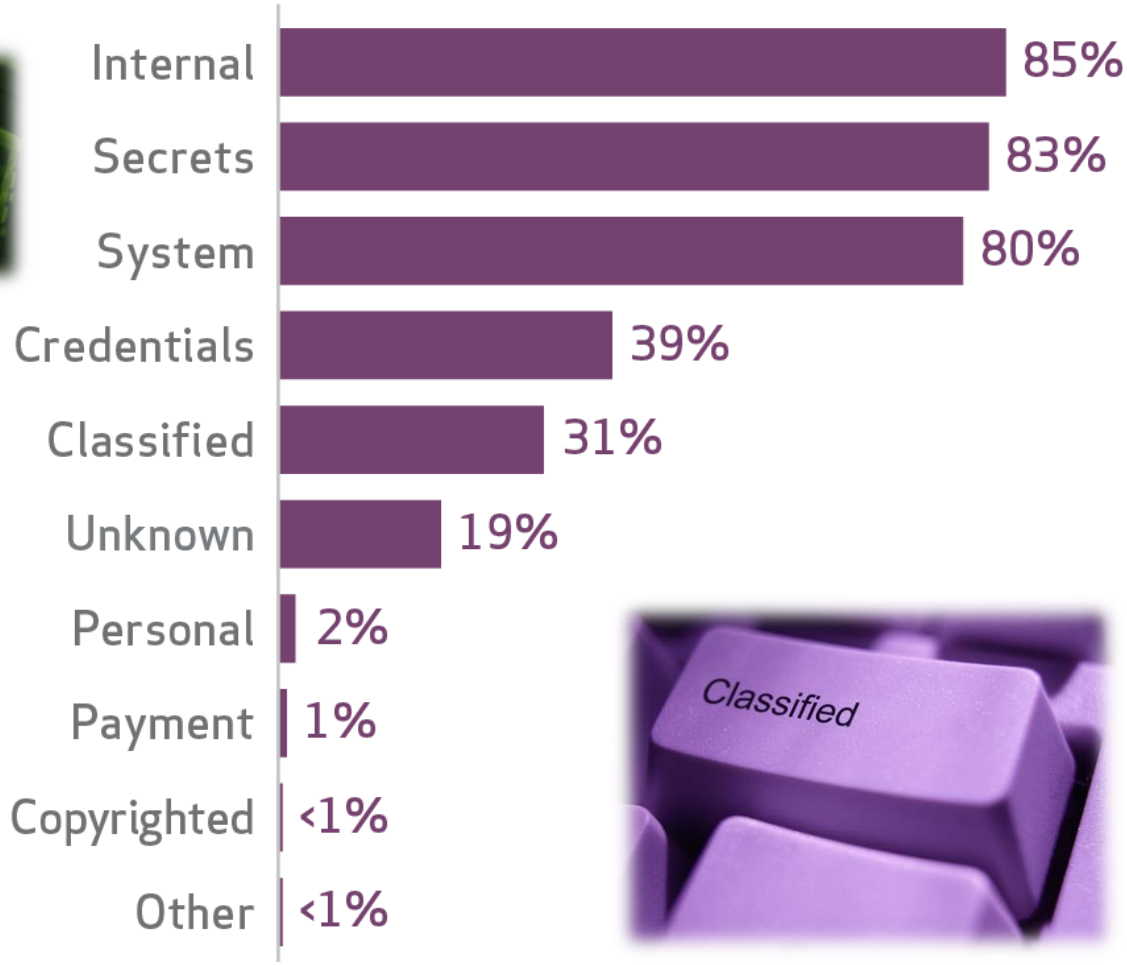
THE INEVITABILITY OF THE CLICK



Attackers compromise sensitive data they're after and credentials along the way

Figure 62.

Variety of at-risk data within Cyber-espionage (n=355)



Discovery methods and times leave a lot of room for improvement

Figure 63.
Top 10 discovery methods within Cyber-espionage (n=302)

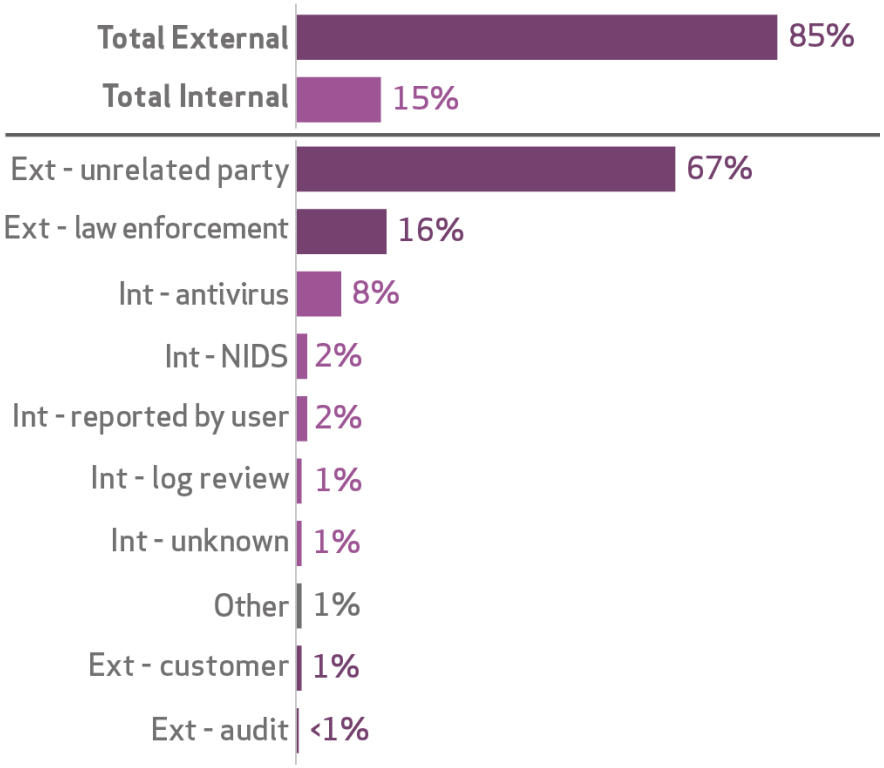
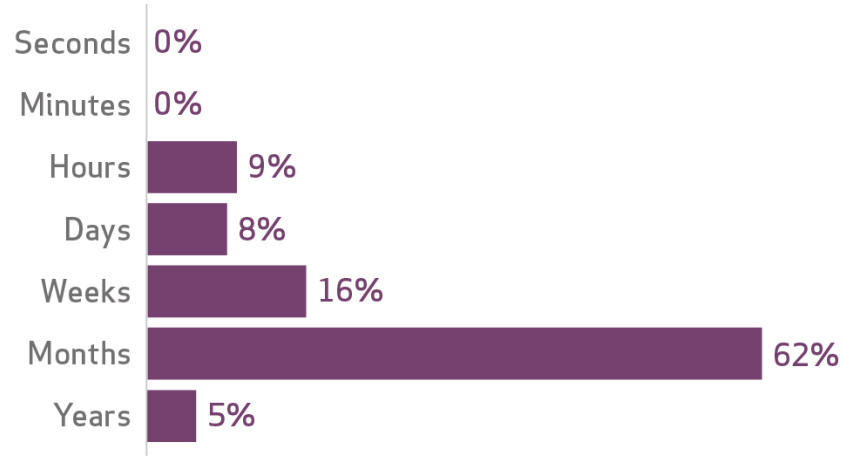


Figure 64.
Discovery timeline within Cyber-espionage (n=101)



Recommended controls for cyber espionage

- Patching
- Anti-virus
- User training
- Network segmentation
- Good logging
- Break the delivery-exploitation-installation chain
- Spot C2 and data exfiltration
- Stop lateral movement inside the network

So what?

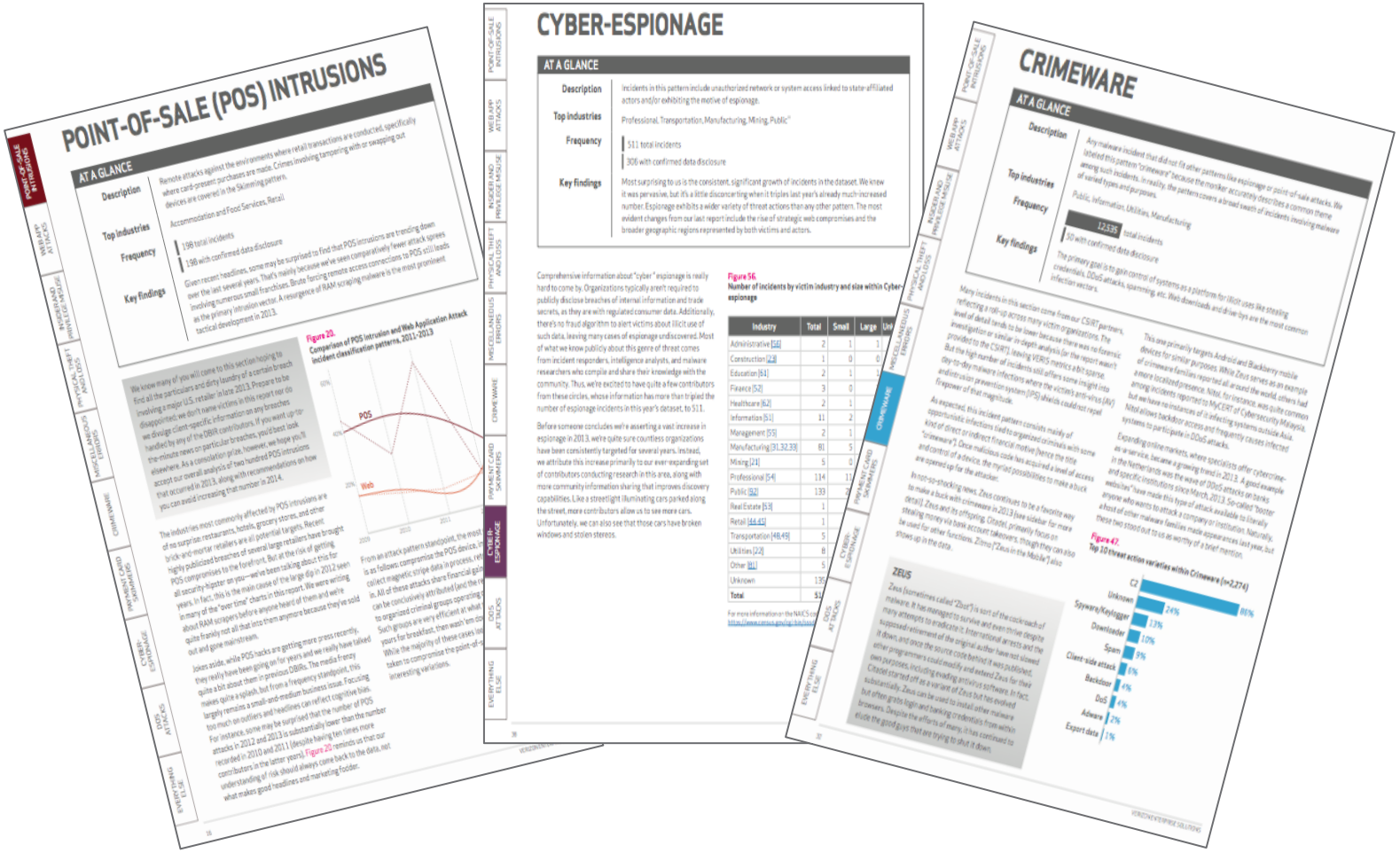
Figure 69.
Critical security controls mapped to incident patterns. Based on recommendations given in this

Critical Security Controls (SANS Institute)		POS Intrusions	Web App Attacks	Insider Misuse	Physical Theft/Loss	Misc errors
Software Inventory	2.4					
Standard Configs	3.1					
	3.2		●			
	3.8					
Malware Defenses	5.1	●				
	5.2	●				
	5.6					
Secure Development	6.4		●			
	6.7		●			
	6.11		●			
Backups	8.1				●	
Skilled Staff	9.3				●	
	9.4					
Restricted Access	11.2	●				
	11.5	●				
	11.6	●				
Limited Admin	12.1	●		●		
	12.2			●		
	12.3	●				
	12.4	●				
	12.5	●				
Boundary defense	13.1					
	13.7	●	●			
	13.10	●				
	13.14	●				
Audit Logging	14.5	●		●		
Identity Management	16.1			●		
	16.12			●		
	16.13			●		
Data Loss Prevention	17.1				●	
	17.6			●		●
	17.9			●		●
Incident Response	18.1					
	18.2					
	18.3					
Network Segmentation	19.4					

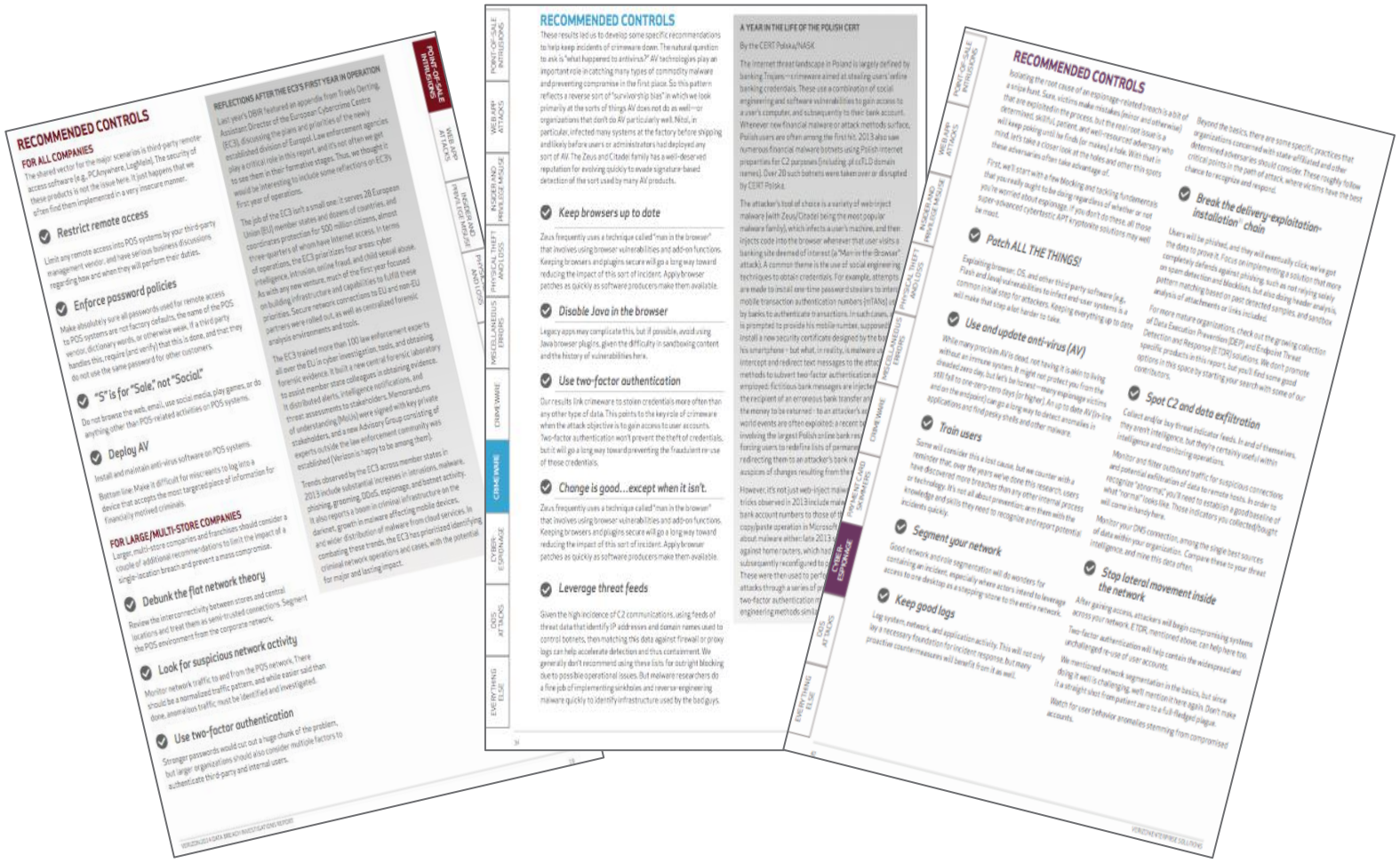
Figure 70.
Prioritization of critical security controls by industry. Based on frequency of incident patterns within each industry and recommendations for each pattern given in this report. The shading is relative to each industry.

Critical Security Controls (SANS Institute)		Accommodation [72]	Administrative [56]	Construction [23]	Education [61]	Entertainment [71]	Finance [52]	Healthcare [62]	Information [51]	Management [55]	Manufacturing [31,	Mining [21]	Other [81]	Professional [54]	Public [92]	Real Estate [53]	Retail [44,45]	Trade [42]	Transportation [48	Utilities [22]
Software Inventory	2.4																			
Standard Configs	3.1																			
	3.2																			
	3.8																			
Malware Defenses	5.1																			
	5.2																			
	5.6																			
Secure Development	6.4																			
	6.7																			
	6.11																			
Backups	8.1																			
Skilled Staff	9.3																			
	9.4																			
Restricted Access	11.2																			
	11.5																			
	11.6																			
Limited Admin	12.1																			
	12.2																			
	12.3																			
	12.4																			
	12.5																			
Boundary defense	13.1																			
	13.7																			
	13.10																			
	13.14																			
Audit Logging	14.5																			
Identity Management	16.1																			
	16.12																			
	16.13																			
Data Loss Prevention	17.1																			
	17.6																			
	17.9																			
Incident Response	18.1																			
	18.2																			
	18.3																			
Network Segmentation	19.4																			

INCIDENT CLASSIFICATION PATTERNS



INCIDENT CLASSIFICATION PATTERNS



Additional information is available

- Download: www.verizonenterprise.com/dbir
- VERIS: www.veriscommunity.net
- Email: DBIR@verizon.com
- Twitter: @vzdbir and hashtag #dbir
- Blog: http://www.verizonenterprise.com/security/blog/

Q&A

Virginia Information Technologies Agency

2014
Datapoint emails

Michael Watson, CISO

August 6, 2014

2014 Datapoint emails

- 2014 Datapoint emails from Archer will be sent shortly from Archer.
- If you have any questions about your agency's score contact CommonwealthSecurity@vita.virginia.gov

- Please note: If you have already submitted a BIA in 2012 or 2013 and have no changes, let Commonwealth Security know so you get credit for reviewing and having a current BIA on file.

2014 Datapoint emails

Questions ??????

Virginia Information Technologies Agency

2014
IS Council Committees

Michael Watson, CISO

August 6, 2014

2014 IS Council Committees

- 2015 IS Conference Committee (Chairs – Rosario Igharas & Marcie Stidman-Stout),
- Information Security as a Percentage and Scope of the IT Budget (Chair – Maurion Edwards),
- IT Security Standards and Policies (Chair - Brian V. Gibbs-Wilson),
- ISO Communication and Knowledge Sharing Website (Chair - Andy Hallberg), and
- IPv6 (Chair - Andrea DiFabio)

IS Council IPv6 Subcommittee

Chair – Andrea DiFabio NSU

IS Council IPv6 Subcommittee

Objectives

The adoption of IPv6, the Internet addressing successor to IPv4, is rapidly growing amongst research networks, Internet service providers, universities and the private sector. Today, many websites provide dual stack IPv4 and IPv6 access, many networks provide native IPv6 communication, cellular carriers provide IPv6 addresses to mobile devices, and vendors ship IPv6 ready products. Some Microsoft products, such as

Exchange email require special installation steps when IPv6 is not enabled.

The purpose of this committee is to empower agency's network and security administrators to make sound decisions when faced with IPv6 questions. This committee will provide current best practices with respect to IPv6, including security implications, concerns and solutions.

IPv6 implementation strategies, specific network configurations, IPv6 product support and deployment, and vendor selection are not within the scope of this document.

IS Council IPv6 Subcommittee

Deliverables

- Provide background information on IPv6 and its current use within the Commonwealth (Possibly through a Commonwealth vide survey)
- Explore the reasons why IPv6 may be necessary, needed or not needed
- Provide resources for agencies wanting to enable or explore IPv6
- Provide resources for agencies wanting to disable IPv6
- Provide resources which may show agencies is their network is IPv6 ready
- Provide resources which may show agencies if their network is running IPv6, whether natively or tunneled
- Analyze security concerns with the use of IPv6
- Provide security solutions and best practices.

IS Council IPv6 Subcommittee

Questions ??????

To join the IS Council IPv6 Subcommittee, please contact: Andrea DiFabio
adifabio@nsu.edu

ISO Communication and Knowledge Sharing Website

Chair - Andy Hallberg

ISO Communication and Knowledge Sharing Website

Questions ??????

To join the ISO Communication and Knowledge Sharing Website Committee, please contact: Andy Hallberg Andrew.Hallberg@abc.virginia.gov

Virginia Information Technologies Agency

Upcoming Events

2015 Security Conference

Save the Date: April 2 & 3, 2015

Location: Crowne Plaza

Future ISOAG

October 1 1:00 - 4:00 pm @ CESC

Topic: Data point requirements, Upcoming changes, Progress report.

ISOAG meets the 1st Wednesday of each month in 2014

IS Orientation

When: Thursday, September 11, 2014

Time: 1:00 pm to 3:00 pm

Where: CESC , Room 1221

Register here:

http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10

Next IS Orientation will be held on December 4, 2014

New Knowledge Center Content

- The following courses have been recently added to Knowledge Center (search for "ISO Academy")

1220 ISO Manual Part 1
1221 ISO Manual Part 2
1222 ISO Manual Part 3
1223 Encryption Techniques

1224 10 Immutable Laws of Security
1225 Pen-Test Paperwork
1226 Wireless Security
1227 Social Engineering

- Ask the Knowledge Center Admin at your agency to pull these courses to your domain.

Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

  Please submit all upcoming events to: **CommonwealthSecurity@VITA.Virginia.Gov**

ISOAG-Partnership Update

IT Infrastructure Partnership Team
Bob Baskette

6 August, 2014

IT INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

Partnership Q & A

Bob Baskette

6 August, 2014

INFRASTRUCTURE PARTNERSHIP

VITA

NORTHROP GRUMMAN

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk